Calhoun: The NPS Institutional Archive

DSpace Repository

Theses and Dissertations | 1. Thesis and Dissertation Collection, all items

1999-06

Migration from netware to windows NT network operating system

Scruggs, Janet E.; Yee, Michael

Monterey, California. Naval Postgraduate School

http://hdl.handle.net/10945/13557

Downloaded from NPS Archive: Calhoun

http://www.nps.edu/library

Calhoun is the Naval Postgraduate School's public access digital repository for research materials and institutional publications created by the NPS community. Calhoun is named for Professor of Mathematics Guy K. Calhoun, NPS's first appointed -- and published -- scholarly author.

Dudley Knox Library / Naval Postgraduate School
411 Dyer Road / 1 University Circle
Monterey, California USA 93943

NAVAL POSTGRADUATE SCHOOL
Monterey, California

19990920 005

THESIS

MIGRATION FROM NETWARE TO WINDOWS NT NETWORK OPERATING SYSTEM

by
Janet E. Scruggs
Michael Yee

June, 1999

Thesis Advisors: Douglas Brinkley
Erik Jansen
Mark Nissen

Approved for public release; distribution is unlimited.

REPORT DOCUMENTATION PAGE

Form Approved OMB No. 0704-0188

Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington DC 20503.

1. AGENCY USE ONLY *(Leave blank)*	2. REPORT DATE	3. REPORT TYPE AND DATES COVERED
	June 1999	Master's Thesis

4. TITLE AND SUBTITLE
MIGRATION FROM NETWARE TO WINDOWS NT NETWORK OPERATING SYSTEM

5. FUNDING NUMBERS

6. AUTHOR(S)
Scruggs, Janet; Yee, Michael

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
Naval Postgraduate School
Monterey, CA 93943-5000

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)

10. SPONSORING / MONITORING AGENCY REPORT NUMBER

11. SUPPLEMENTARY NOTES
The views expressed in this thesis are those of the authors and do not reflect the official policy or position of the Department of Defense or the U.S. Government.

12a. DISTRIBUTION / AVAILABILITY STATEMENT
Approved for public release; distribution unlimited.

12b. DISTRIBUTION CODE

13. ABSTRACT *(maximum 200 words)*

Migration from an existing information technology system to a new system presents many managerial challenges. There are technological challenges associated with running the old system, maintaining data integrity and bringing the new system online all without seriously impacting daily operations. There are human factors to consider like resistance to change and conflict management. In addition, organizational issues like management support and cross-functional communication channels need to be addressed. This thesis reviews the technical migration from an operational NetWare network to Windows NT completed at the Defense Manpower Data Center (DMDC) in Monterey, CA. The DMDC case presents a typical set of issues that an IT manager is likely to face when implementing technology-driven change. Technical, human and organizational factors of technical change are discussed. A list of lessons learned and a set of technical management guidelines are derived from analysis of the DMDC case. Details of Windows NT 4.0 and 5.0 features are included.

14. SUBJECT TERMS	15. NUMBER OF PAGES
Networking operating systems, change management, project management	127
	16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	18. SECURITY CLASSIFICATION OF THIS PAGE	19. SECURITY CLASSIFI- CATION OF ABSTRACT	20. LIMITATION OF ABSTRACT
Unclassified	Unclassified	Unclassified	UL

NSN 7540-01-280-5500

Standard Form 298 (Rev. 2-89)
Prescribed by ANSI Std.

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release; distribution is unlimited

MIGRATION FROM NETWARE TO WINDOWS NT NETWORK OPERATING SYSTEM

Janet E. Scruggs
B.S., University of Maryland, 1991
Michael Yee
A.B., University of California, Berkeley, 1971

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN INFORMATION TECHNOLOGY MANAGEMENT,
MASTER OF SCIENCE IN INFORMATION SYSTEMS

from the

NAVAL POSTGRADUATE SCHOOL
June 1999

Author: [redacted]
Janet E. Scruggs

[redacted]
Michael Yee

Approved by: [redacted]
Douglas Brinkley, Thesis Advisor

[redacted]
Erik Jansen, Thesis Advisor

[redacted]
Mark Nissen, Thesis Advisor

[redacted]
Reuben T. Harris, Chairman
Department of Systems Management

[redacted]
Dan Boger, Chairman
Information Systems Academic Group

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

Migration from an existing information technology system to a new system presents many managerial challenges. There are technological challenges associated with running the old system, maintaining data integrity and bringing the new system online all without seriously impacting daily operations. There are human factors to consider like resistance to change and conflict management. In addition, organizational issues like management support and cross-functional communication channels need to be addressed. This thesis reviews the technical migration from an operational NetWare network to Windows NT completed at the Defense Manpower Data Center (DMDC) in Monterey, CA. The DMDC case presents a typical set of issues that an IT manager is likely to face when implementing technology-driven change. Technical, human and organizational factors of technical change are discussed. A list of lessons learned and a set of technical management guidelines are derived from analysis of the DMDC case. Details of Windows NT 4.0 and 5.0 features are included.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

I. INTRODUCTION.....1

A. BACKGROUND.....1

B. PURPOSE.....3

C. RESEARCH QUESTIONS.....4

D. SCOPE.....4

E. METHODOLOGY.....5

F. ORGANIZATION OF STUDY.....5

G. BENEFIT OF STUDY.....7

II. HISTORY OF NETWORK OPERATING SYSTEMS.....9

A. OVERVIEW.....9

B. NOVELL HISTORY.....10

C. MICROSOFT (LAN OS) HISTORY.....13

D. CHAPTER SUMMARY.....16

III. TECHNICAL COMPARISON OF NETWARE AND NT.....17

A. BACKGROUND.....17

B. LAN OS CONFIGURATIONS.....20

C. COMPARISION NETWORK ELEMENTS AND SERVICES.....21

1. Connectivity.....21
2. File Systems and Services.....22
3. Print Services.....25
4. File Transfer.....26
5. Application Server.....27
6. Directory Services.....30
7. Security.....32
   a. *C2*.....33
   b. *Rights, Permissions, Access Lists*.....34
   c. *Vulnerabilities*.....35
8. Remote Access.....40

9. Network Administration.....40
10. Internet Access.....41

D. INTEGRATION ISSUES WHEN USING BOTH NOVELL AND NT.....43
1. Client.....43
2. NIC Driver.....44
3. Directory Synchronization.....44
4. Value.....46

E. NT IMPLEMENTATION CONSIDERATIONS.....46

F. KEY NT AND NETWARE DIFFERENCES.....47

G. ADDITIONAL NEW FEATURES.....48

H. FINAL – MARKET SHARE COMPARISON.....50

IV. MANAGING TECHNOLOGY-DRIVEN CHANGE.....53

A. INTRODUCTION.....53

B. WHY MANAGE CHANGE?.....57
1. Velocity of Change.....59
2. Critical Changes Impacting IT Managers.....60
3. Productivity Paradox.....63
4. Magic Bullet Thinking.....64
5. Summary of "Why".....65

C. HOW TO MANAGE CHANGE.....66
1. Getting Started.....66
2. Seven-Step Change Process.....72

D. Summary of "How".....76

V. NETWARE TO NT CONVERSION CASE STUDY.....77

A. THE ORGANIZATION: DEFENSE MANPOWER DATA CENTER (DMDC).....77

B. NT 4.0 AT DMDC.....77
1. NT Business Drivers.....79
2. The Plan.....79
3. What Happened.....80
4. Inherited Problems.....84
5. Implementation Procedures.....86

VI. ANALYSIS OF DMDC NETWARE TO NT MIGRATION....93

A. ORANIZATIONAL FACTORS....93
1. Change Management....93
a. Forces Driving Change....95
b. Resistance to Change....95
c. Corporate Culture....97
d. Developing Enabling Structures....98
e. *Change Management Applies to Everyone*....99
f. Be Proactive in Training....99
g. IT Philosophy....100
h. Management Support....101
2. Conflict Management....101
a. Understanding the situation: Cowboys versus the Nazis....102
b. Thomas Conflict Resolution....103

B. TECHNICAL FACTORS....106
1. The Novell Factor....106
2. Microsoft Caveats....107
3. Marketing hype....108

C. PROJECT MANAGEMENT FACTORS....109
1. Underestimating Resources....109
a. Time....109
b. Personnel....110
2. No Model....111
3. Lack of Taining....111
4. Coordination....112
5. Implementation....112
6. Management support....113

D. CHAPTER SUMMARY....113

VII. LESSONS LEARNED AND CONCLUSION....115

A. NETWARE TO NT LESSONS LEARNED AT DMDC....115
1. Use One NOS....115
2. Allocate Sufficient Time....116
3. NT Requires More Hardware....116
4. NT Requires Special Expertise....117

B. PROJECT MANAGEMENT RECOMMENDATIONS....117
1. Get Management Support....117
2. "It's the People, Stupid."....117
3. Communicate, Communicate, Communicate....118

4. Understand the Environment.....119
5. Plan the Project.....119

C. CONCLUSION.....121

LIST OF REFERENCES.....123

INITIAL DISTRIBUTION LIST.....127

I. INTRODUCTION

A. BACKGROUND

How does an organization that is in a state of continual change use a technology that is in a state of rapid advancement? The Department of Defense (DoD) must respond to changes in budget, political, foreign policy and national security issues. Put another way, DoD is in a constant state of flux. DoD uses information technology (IT), which continually changes in response to technological advances in hardware components and market demand for improved ways of managing information.

IT is changing more rapidly than any technology in history. Our ability to produce tools, which employ technology advances, and then to assimilate those tools into our culture is, however, a much slower, more frustrating process. Change brings advancement in capabilities, but rapid technology change also presents IT managers with a huge update and integration challenge. Combine the rapid rate of technology advancement with the variety of IT vendor hardware, software and protocol standards, and achieving interoperability (i.e., making things work together) becomes almost impossible in many situations.

Joint Vision 2010 (CJCS) recognizes information superiority as the critical element needed to achieve and maintain military dominance in the 21st century. The DoD must resolve IT interoperability issues in order to assure information superiority. In addition to concerns over making things work together, the shrinking defense budget demands that DoD work smarter. Operation costs are higher to train people to use and maintain a variety of hardware and software products. DoD can no longer afford the

higher operations costs and lost productivity costs brought about by supporting a variety of IT products.

The Navy is attempting to meet this interoperability challenge with the IT21 initiative outlined by Admiral Archie Clemins. IT21 provides the Navy with a set of hardware, software and protocol standards aimed at eliminating the problems caused by the use of IT products that cannot inter-operate. Although many would argue that there is no "one size fits all" standard set, most agree that standards are necessary for complex IT systems to run efficiently. A standard should be comprehensive enough to handle the majority of requirements and flexible enough to allow for the exceptions.

IT21 specifies a list of hardware and software standards that must be implemented at fleet activities by December 1999. In the area of network operating systems, Novell Corporation's NetWare has been the recognized industry standard for the past decade. However, Microsoft's Windows NT network operating system is rapidly emerging as the new industry standard, and Windows NT 4.0 is identified as the network operating system standard for IT21. While the initial IT21 directive addresses fleet activities, shore commands should carefully consider adopting the standards. Shore commands have the same interoperability and cost issues that the fleet faces, and as important, the shore commands must be able to seamlessly communicate with the fleet, their primary customer.

Identifying a set of standards is only the first step in addressing the interoperability challenge. A plan to implement those standards must then be developed and executed effectively. The organization's social system and the environment in which the organization operates must also be considered. Any plan to implement a

technological change must include steps to meet with internal and often external resistance to that change. "Resistance is a normal part of the change process; in fact, there can be no real change without resistance." (Beckhard, Harris, 1987) Expecting, understanding and planning for change resistance is crucial to the successful implementation of a technological change. Many projects have suffered serious schedule setbacks or become derailed entirely when project planners forgot to consider the resistance to change factor. Change management issues, which are really people issues, must be included in any IT implementation plan and are particularly important when the new technology standards require replacing a well-known system (e.g., Novell) with a new system (e.g., Microsoft).

B. PURPOSE

The objective of this thesis is to identify key considerations when migrating an operational NetWare network to Windows NT. A case study of the NetWare to NT conversion work done at the Defense Manpower Data Center (DMDC) in Monterey, California is conducted to identify important issues to consider when beginning the conversion process. This thesis addresses both technology and people issues. Technologically, it covers the difference in implementation approaches of NetWare and Windows NT, compatibility issues, hardware and software requirements. Organizationally, it focuses on change management, personnel and training requirements. The goal is to capture and formalize a general set of lessons learned to help future operational IT managers with this transition.

C. RESEARCH QUESTIONS

- Primary: What lessons can be learned to guide future managers in their conversion to an IT21 network infrastructure?
- Secondary:
  1. What are the major components of a network operating system, and how have they evolved in the past ten years?
  2. How do NetWare and Windows NT differ in functionality, and what network administration standard operating procedures must be adapted to deal with those differences?
  3. What change management issues should be considered when planning a technical change?

D. SCOPE

The scope of this thesis includes: (1) a review of network operating system architectures, (2) a review and contrast of NetWare and Windows NT network operating systems, (3) an evaluation of the NetWare to Windows NT migration process at the DMDC in Monterey, CA (4) a review of change management issues to consider in a technical implementation (5) a list of NetWare to NT "lessons learned" at the DMDC. The thesis concludes with an outline of NetWare to NT planning and conversion issues and proposes recommendations for successful implementation of Windows NT.

E. METHODOLOGY

The methodology used in this thesis research consists of the following steps:

1. Conduct a literature search of books, magazine articles, CD-ROM systems, and other library information resources.

2. Conduct a thorough review of NetWare and Windows NT hardware requirements, system management requirements, compatibility issues, and standards.

3. Use an analytical framework from theory or practice to guide the case study of the NetWare to NT conversion process being undertaken at the Defense Manpower Data Center (DMDC).

4. Generalize from the case study, and identify issues to address when planning a NetWare to NT conversion.

The literature search and review of NetWare and Windows NT provides information to answer the secondary research questions. The analytical framework used to guide the case study of DMDC's NetWare to NT conversion is Stewart L. Stokes, Jr.'s Seven-Step Change Process. (Stokes, 1991) Generalization is accomplished through identification of DMDC technology and people factors that are common across other organizations and systems.

F. ORGANIZATION OF STUDY

Chapter II begins with a review of what a network operating system (NOS) does. A synopsis of Novell and Microsoft history is presented to provide insight into the development paths of each NOS product. Chapter II provides the answer to the research

question: What are the major components of a NOS, and how have they evolved in the past ten years?

Chapter III is a technical comparison of NetWare and Windows NT. Functional and network administration differences are outlined, and recommendations to deal with those differences are made.

Chapter IV addresses the human side of technology-driven change. The Seven-Step Change Process, developed by Stewart L. Stokes, Jr., is a methodology for implementing technological change more effectively. The Seven-Step Change Process, outlined in this chapter, provides a practical approach to change management. In addition to the change process model, this chapter focuses on what systems professionals and managers should know as they introduce, manage and cope with technological changes.

Chapter V presents a case history of DMDC's migration from NetWare to Windows NT 4.0. The chapter provides an overview of what the DMDC does and how its network is configured. DMDC's conversion and implementation plan is reviewed, and a discussion of how well the plan met reality follows. What did and what did not work in DMDC's technical migration is included.

Chapter VI is an analysis of the DMDC case study. The Seven-Step Change Process analytical framework is used to review DMDC's technical migration experience. The analysis addresses pre-conversion decisions, conversion planning, implementation, training and user acceptance.

Chapter VII provides a list of lessons learned and recommendations derived from the Chapter VI analysis, and presents the key conclusions of the thesis. The recommendations provide insight on what to do and problem areas to avoid during a conversion from NetWare to NT.

G. BENEFIT OF STUDY

This study provides a guideline for planning and implementing a conversion from NetWare to Windows NT network operating system. It identifies problems that may be encountered in the migration process, and recommends ways to avoid or resolve those problems. The case study provides detailed information pertaining to an IT21 conversion and the study generalizes important lessons learned to help other organizations' technological conversions.

THIS PAGE INTENTIONALLY LEFT BLANK

II. HISTORY OF NETWORK OPERATING SYSTEMS

A. OVERVIEW

What is a network operating system (NOS) and what does it do? Very simply, the NOS is the program that controls the network. At the most basic level, it facilitates user-to-user communication and controls the sharing of resources like files and printers. The NOS accomplishes this by coordinating file access and file sharing, managing server memory, managing data security, scheduling tasks for processing, coordinating printer access and managing inter-network communications. File and print services were the two primary features of the early NOS programs, developed over a decade ago. Today's network requirements are much more demanding. Consequently, modern NOSs have developed into sophisticated platforms designed to support functions such as e-mail servers, fax servers, database servers to provide a central location for corporate data, and communication servers to act as gateways between desktop workstations and company mainframes. Many local area network (LAN) customers also require remote access servers to allow users to dial into the network from remote locations, telephony servers to connect LANs to Public Branch Exchanges (PBXs) and supported automated call centers, imaging servers and even online transaction processing (OLTP) servers. As LANs have grown in size and complexity, built-in LAN management tools have become a requisite NOS application for network managers. Many of the applications running on LAN servers are mission critical and must be protected, which demands that a NOS also provide fault tolerance and network security capabilities. In other words, a NOS must

provide and manage all of the capabilities earlier corporate mainframes did plus the latest advancements in computing technology.

B. NOVELL HISTORY

Founded in 1983, Novell's NetWare has been the leading LAN operating system for over a decade. Novell acquired its dominant market share by providing support to multiple vendors including PCs, Macs and UNIX. "Because Novell's primary focus has been on LAN operating systems, the company has a thorough understanding of customer requirements and has been able to stay in step with changing network requirements." (Korzeniowski, 1996) Novell has a lot of third-party and reseller support as well as many technicians who thoroughly understand the installation and operation of NetWare LANs.

Early on, Novell understood that speed was important to network customers. "To make its file and print functions fast, Novell did not include common OS functions such as a protected mode, a preemptive job scheduler, and comprehensive memory management." (Korzeniowski, 1996) The strategy to focus on one product, make it faster than the competition and support all vendors worked well for Novell for many years.

Installation and maintenance of networks became simpler and less expensive, allowing the number of network customers to grow. As Intel Corporation's microprocessor became more powerful and less expensive, business and government began to shift many core applications to LAN servers. "A new category of LAN OS features emerged: Application servers. These servers are the central control points for specific common functions, which users share." (Korzeniowski, 1996) The LAN world had changed and Novell's original strategy needed to be revisited.

Originally, network applications ran on a machine other than the NetWare server, and thus administrators had to deal with a second OS connected to the Novell network servers. If the application did not support NetWare's integrated packet exchange (IPX) protocol, the network administrator would have to deal with two operating systems and two protocols when attempting to resolve a problem or implement routine system maintenance. In 1989, Novell introduced NetWare loadable modules (NLMs) to enable organizations to run applications on a NetWare server. This significantly reduced the network administration burden.

Customer interest in NLMs quickly grew. There are NLMs to connect NetWare LANs to IBM mainframes, NLM versions of major LAN database management systems, and a Lotus Notes GroupWare NLM. FAX, telephony and imaging NLMs are also available. NetWare 4.1 includes a symmetric multiprocessing (SMP) NLM that allows SMP-aware applications to run on multiple processors. This is an important feature to many organizations running resource-intensive, core applications on LAN servers.

Even with the enthusiastic market for NLMs, there are some limitations. NetWare was not designed as a general purpose OS. Therefore, NLM application developers have to work directly with the complex NetWare OS. There are few application development and programming tools available for NLM development. Consequently, NLM development is a difficult process that takes most software companies more than a year to complete. (Korzeniowski, 1996)

Novell made some serious strategic missteps during the 1990s. The company abandoned its original plan to focus exclusively on the NOS market and began efforts to compete in the desktop application market. The desktop was the customer's entry to the

network and Novell planners felt that the company should be in that market. Novell tried to merge with Lotus Development Corporation, but the talks ended when the two companies could not agree on the makeup of a board of directors and leadership of the group venture. In 1990, Novell bought Digital Research, Inc.'s DR-DOS, the only PC OS competitor to MS-DOS. The product never gained a great deal of market acceptance, and Novell terminated the product in late 1994.

Novell decided to gamble on UNIX as a possible way to get into the desktop arena. They began collaborating with UNIX Systems Laboratories, a UNIX development house based in Summit, NJ, on UNIXWare, a PC desktop version of UNIX, which connected users to NetWare servers. In 1992, Novell purchased UNIX Systems Laboratories and began development of SuperNOS, which would combine NetWare's file and print services with UNIX's application server capabilities. The idea sounded like a good opponent to the soon to be released Windows NT. Unfortunately, Novell did not have the UNIX expertise to give the project any real momentum. Novell gave up on its UNIX development and sold the project to two companies already established in the UNIX environment. Novell purchased UNIX Systems Laboratories for $360 million and sold the assets for $60 million. The UNIX gamble lost Novell money and degraded its customers' confidence in the company's leadership.

Novell jumped into the desktop application market in 1994 with the acquisition of WordPerfect Corporation's office suite for $1 billion. They also purchased a spreadsheet application from Borland International, Inc. Novell did not realize that they purchased these products near the end of their life cycle when customers were beginning to switch over to Microsoft alternatives. That lack of understanding, once more, cost the company

in dollars and in customer confidence. Novell sold WordPerfect for $124 million plus royalties less than two years after it was acquired.

With its AppWare product, Novell tried to become a player in the application development area. AppWare was a set of Object Oriented Programming (OOP) tools with a modular architecture that allowed programmers to string together objects to create programs. The AppWare effort suffered from the same problems that the Novell UNIX development effort did. The company did not have the expertise and rather than train or purchase the expertise, Novell focused on what it knew, NetWare. In September 1994, Novell began to extricate itself from the application development area.

In 1995, Novell also found itself bowing out of a venture with Apple Computer, Inc., and IBM to support emerging OpenDoc specifications. "OpenDoc is a set of specifications designed to enable companies to more easily link objects on a network." (Korzeniowski, 1996)

"Novell stumbled badly earlier in the decade, blowing a near-monopoly of the LAN server market with an ill-conceived attempt to challenge Microsoft on the desktop. This two-front war alienated independent software vendors (ISV), confused users and diverted resources and attention away from Novell's core network-services business." (Breidenbach, 1999) It seems that Novell finally decided to shift its strategy away from direct competition with Microsoft and back to doing what it knows which is providing comprehensive networking services.

C. MICROSOFT (LAN OS) HISTORY

Microsoft's story could be described as the opposite of Novell's. Microsoft, founded in 1975, became the leader in the PC desktop OS market, very successful with

its desktop productivity tools, and it also fared well in the application development tool arena. Microsoft's history in the LAN OS world had shown little success until Windows NT.

Microsoft made two failed attempts at getting into the NOS market prior to NT. In 1984, Microsoft worked with IBM to develop MS-Net. IBM did most of the development, because Microsoft had limited networking expertise. IBM sold MS-Net as PC Network and later PC LAN and 3Com marketed it as Ethershare. MS-Net was a 16-bit OS that did not offer the speed that NetWare offered. Even with IBM's backing, MS-Net never achieved more than 10 percent of the market share. In 1987 Microsoft introduced LAN Manager, a NOS that ran on MS-DOS and OS/2. IBM, Digital Equipment Corporation (DEC) and Hewlett-Packard Company (HP) all sold versions of LAN Manager.

Unfortunately for LAN Manager, a dispute over what should be the successor to MS-DOS alienated Microsoft and IBM. Initially, the two companies agreed that Windows was a stop-gap replacement measure for MS-DOS to prevent the PC from loosing market share to Apple Corporation's Mac. DOS was at the end of its life-cycle and the PC platform needed a new OS that would better meet emerging requirements like integrating desktop and server functions. OS/2 was to be the replacement for MS-DOS. It provided multitasking and multithreading capabilities. Unfortunately for IBM, the market did not accept OS/2. The new OS required expensive hardware upgrades and there were few applications available to run on it. Customers were willing to upgrade to Windows, because it was easier to do. DOS was still the underlying OS, and there were many applications available. IBM insisted that OS/2 was the correct technical direction.

Given the success of Windows, Microsoft disagreed. IBM split with Microsoft over this dispute. When IBM left, LAN Manager lost its most important backer and never gained momentum.

Novell easily defeated the first two NOS challenges by Microsoft, but many believe Microsoft's third attempt has been a charm. The idea for NT began in 1988 when Microsoft technology guru, Nathan Myhrvold, convinced Bill Gates of the need for a portable OS to run on reduced instruction set computer (RISC) chips to compete with UNIX. At that point no one knew if the Intel-based machines would continue their growth as enterprise computing platforms or if they would lose out to RISC machines. Microsoft wanted to hedge its bets that if the Intel bubble burst, it could compete directly against UNIX on a RISC platform.

Microsoft hired David Cutler, a well-known DEC virtual memory system (VMS) programmer to lead the RISC project. Cutler created Windows New Technology (NT). The OS is a symmetric multi-processing (SMP) system that supports file, print and application services. Microsoft dedicated over six years and $600 million to the development of Windows NT Server. It missed the initial projected shipment date by more than a year, but NT was formally announced on May 14, 1993 at Windows World in Atlanta and was released in June of 1993.

"Unlike NetWare, Windows NT was designed to operate as an application server. There is simple, tight connectivity between its Windows operating systems and the Windows NT Server." (Korzeniowski, 1996) Given the shift in customer expectation from file and print sharing to application server capabilities, this put Microsoft in a good position to finally capture a large share of the NOS market.

D. CHAPTER SUMMARY

The following quote from a *PC Magazine* article best sums up how network operating systems have evolved in the past decade:

> What once was a single product providing fast file and print services is now best considered part of an extended family of products providing messaging, remote access, management, Internet and intranet connections, and other essential network services. When it comes to choosing a NOS today, network services and the flexibility to operate within a multi-OS, multi-platform environment are more important considerations than file and print performance. (Derfler & Pompili, 1997)

NetWare's position as the leading NOS vendor is losing ground to Windows NT. Novell's strategic blunders cost it dollars and market share. Many organizations have already converted or are planning to convert to NT, because they fear that Novell will continue to lose customers and will eventually go out of business. A big advantage for Microsoft is the number of applications that are written for Windows NT. NetWare NLM development is complex and slow, which limits the number of applications that are built to run on NetWare. Application availability and the perceived instability of the Novell Corporation are two significant advantages for Microsoft in the battle to win the NOS market.

In Chapter III we look at the functional and network administration differences in NetWare and NT.

III. TECHNICAL COMPARISON OF NETWARE AND NT

A. BACKGROUND

Chapter II introduced networking concepts and described Novell and Microsoft history. Where Chapter II contrasts the NOS development history of Novell and Microsoft, this chapter contrasts the features and implementation methods of NetWare and Windows NT. In addition to contrasting the two products, a section on integrating NetWare and NT is included. It is intended to provide "real life" implementation details that are often omitted from generalized technical articles and books. This thesis provides a means to share the NT implementation problems that DMDC found.

Originally, this chapter was to focus on technical information obtained from the NetWare to NT 4.0 migration experience at DMDC. However, information obtained at several NT sessions at the 1999 Networld + Interop (N+I) just prior to publishing this thesis changed some of the message. Microsoft is addressing many of the NT shortcomings that were present when the authors began writing this thesis. As is often the case with software release promises, some are partial fixes and some are immature plans to resolve a problem, but there is a definite direction toward addressing many of the authors' complaints against NT 4.0. This is a lesson in itself. The industry is changing so fast that by the time an experience is documented, it may already be obsolete. Chapter IV discusses some of the problems associated with the current velocity of change in the IT world. Where applicable, the authors have incorporated NT 5.0 changes that address a shortcoming in NT 4.0.

The 1999 N+I conference held a "NOS shootout" between NetWare and NT. Comments made in that session highlighted the current market situation for Novell and NT. Microsoft continued to tout lower cost, ease of use and more features and benefits through tying the operating system to its dominant Office application product line. Drew Major, one of the original Novell pioneers, who often leads the technology directions discussions at Novell BrainShare and is currently Novell's chief scientist, represented Novell. Drew said Novell is not a general purpose OS. He said it is now a specialized niche product needed to provide things like cache for Internet, security services with its BorderManager products and directory services with Netware Directory Services (NDS). Novell claimed its products to be superior and faster than Microsoft's and that there is room for Novell somewhere in the LAN. The use of the word niche and positioning Novell as a product to fit "somewhere in the LAN" clearly shows Novell's recognition and acceptance that NT has become the predominant LAN OS in the today's market. As Microsoft improves its products and provides capabilities similar to Novell, it will be hard to justify the expense and complexity involved in integrating both technologies. This news reinforces the Navy's IT21 concept.

Making matters worse for Novell, after N+I, it was announced that packaging and licensing of Netware 5.0 will no longer include Novell's Netware Directory Services (Baltazar, 1999, p. 59). For many organizations, Novell's NDS is the key reason to use NetWare as the enterprise NOS for file and print services. An upgrade to NetWare 5.0 is attractive, because it uses the Internet standard native Transmission Control Protocol/Internet Protocol (TCP/IP) for all function calls and network components instead of Novell's proprietary Internet Packet Exchange/ Sequenced Packet Exchange

(IPX/SPX) protocol. (Harbaugh, 1998) However, unbundling NDS and having to purchase it separately is a large disincentive to buy NetWare 5.0. The Novell Zenworks, technology to distribute and manage software delivery and configuration, is also not included in the NetWare 5.0 package (NOS Crossroads, PC Week, May 10, 1999). Novell's upgrade policy already makes it expensive to upgrade, and unbundling its most competitive functions from the NOS adds another reason for a Novell site to stop using NetWare as its primary LAN OS.

Both Microsoft and Novell are in the process of upgrading their network operating system products. At the time of the writing of this thesis, NetWare 5.0 is generally available (GA). NT 5.0, also called Windows 2000 is in its third and final beta release, and Microsoft has announced it will be GA in late Fall 1999. For completeness and to provide value for the near future, capabilities of both NT 5.0 and NetWare 5.0 are included in the following technical comparison. Although the information on NT 5.0 is from a beta release and can still change with testing, the items and issues represent the best information available at the writing of this thesis. The new NT release contains many important features, particularly the Active Directory Services, and should be considered here.

NetWare's services, such as NDS, are more mature than comparable services in NT. NT is very complex, and many of its functions are still new and evolving. There are more than 30 million lines of code in NT 5.0. The increased complexity also means increased chances of problems with operation and reliability of the code. This causes many to question the stability of the NT 5.0 platform.

B. LAN OS CONFIGURATIONS

A network consists of computers connected together. A simple network model is a peer to peer network. In such a network, there is no centralized server. Instead, each computer or host talks with other hosts to share information and exchange roles as client and server. (Berg, 1998, p. 15) Novell Lite uses the peer to peer model (Nowshadi, 1994, p. 16). Windows 95 and Windows NT workstation have peer to peer network capabilities (Boyce, 1996, p. 350).

A more advanced model of networking is client server. In the client server model, network functions and services are centralized on servers. Client workstations obtain network services by authenticating via a centralized login process that verifies the workstation is in a membership repository. The memberships retain security data about the information that can be accessed on the network and about permissions granted to perform various network functions. NetWare and Windows NT use the client server model. Unless you have a very small network of less than ten workstations, avoid peer to peer networking. (Berg, 1998, p. 15)

The centralized server model includes a number of services. As mentioned in Chapter II, these services include connectivity, file, print, file transfer, application, directory services, security and remote access. In addition to these basic LAN OS services, there are three important NOS functions to be considered. Ease of network administration, ease of implementation and Internet connectivity are key areas that need to be well understood by the technical staff.

C. COMPARISION NETWORK ELEMENTS AND SERVICES

1. Connectivity

Network connectivity is accomplished via a network interface card (NIC). Data from the personal computer bus is converted from a parallel to a serial signal to allow travel across the transmission media. The driver for the network card provides the software interface to do this conversion. (Berg, 1998, p. 199)

For Novell, the driver is the Open Data-Link Interface, ODI (Lawrence, 1995, pp. 967-968). For Microsoft, the Network Driver Interface Specification (NDIS) is the standard that connects the network transport protocol and the data link layer network adapter driver (Berg, 1998, p.88).

The NIC can have 8-bit, Industry Standard Architecture (ISA), 16-bit Extended Industry Standard (EISA), 32-bit Micro Channel (MCA), or 32-bit Peripheral Component Interconnect (PCI). PCI is most common for Pentium based machines. The NIC can support different network standards. For example, both 10BasedT and 100BaseT implementations of the 802.3 Ethernet standard, defined by the Institute of Electrical and Electronic Engineers (IEEE), are supported. These are the ones you will most likely encounter. There are NICs for other topologies such as Token Ring, defined by the IEEE 802.5 and also Fiber Distributed Data Interface (FDDI) standard definition NICs for fiber network architectures. For each new technology, such as the gigabit ethernet, the industry works towards defining standards and a new NIC to support the technology. (Berg, 1998, p. 206)

You can never have too large a bus or too much bandwidth. The authors recommend that the current most cost-effective solution, is a 32-bit PCI NIC that is

software configurable and has auto-select 10/100. Connect to a switch or hub connection for 100BasedT. Make sure the NIC has the drivers for your operating system. For NT, check the Windows NT Hardware Compatibility List (HCL). Novell used to make hardware and NIC cards, the NE2000. Any NIC that is NE2000 compatible will work for Novell. For server hardware companies such as COMPAQ, use of their NIC is recommended.

2. File Systems and Services

A NOS provides file storage services. The ability for people to share information across the network is a fundamental NOS function. NetWare and NT have different file storage characteristics, and Microsoft uses different file systems for its operating systems. File access permissions provide file security, and will be discussed in the security and administration sections. This section covers file storage characteristics.

The file allocation table system, FAT, has existed since the days of DOS. Information is stored in a group of sectors called clusters based upon available space. The FAT tracks the file name and the first cluster. Each location has the first sector of the next cluster where the data are stored in a linked list fashion. FAT has a disk size limitation of 2 gigabytes. (Boyce, 1996, pp. 210-218)

Microsoft provided additional systems such as VFAT and FAT32, available for Win98 clients, to overcome disk limitations. NT provides a more secure file storage system via the new NT file system (NTFS).

NTFS was designed specifically for NT and has a number of performance, reliability and security advantages. NTFS provides faster throughput than FAT for small files. NTFS uses a master file table (MFT). The MFT contains data about the file

including name, security descriptor and other file attributes. The MFT entry is stored within the data file. If the entire file cannot be stored contiguously, additional storage runs or extents are assigned. The MFT stores the locations of the file extents. For larger files, NTFS does add some overhead. (Jennings, 1996, p. 99)

When NT was first released, there were discussions about the advantages and disadvantages of NTFS and whether or not to use it. In part, the debate stemmed from the fact that, in the early days, NT drivers where not available for many devices. Also, early releases of NT crashed a lot and many users kept a DOS FAT partition to allow them to bring the machine up for repair with a DOS boot floppy.

NT 4.0 provides a reliable means of emergency repair with the emergency recovery disk (ERD). NT 4.0 capacity is a theoretical 16 exabytes for one volume. There is practically no limit on the number of files per unit and the largest single file can be 16 exabytes (Strebe, 1997, p. 149).

Today, most NT network administrators agree that the security features of NTFS make it the best choice for the file system on an NT server (Strebe, 1997, pp. 148-149). Use Redundant Array of Inexpensive Disks (RAID), which NTFS supports, and format the entire drive under NTFS for the server (Strebe, 1997, p. 96).

Service Pack 4 (SP4) for NT 4.0 uses a different NTFS format. You should carefully consider whether to apply. Since the format is different, once SP4 is installed, it cannot be reversed (Tittel, 1999).

NT 4.0 has no easy way to limit users use of server disk space. In SP4 there is a way to control and limit how much server disk space a user can have with the Proquota utility. Proquota, however, can only limit the maximum amount of allowed disk space

per user. Some third party disk quota managers can also limit size of the user's files. Proquota works only with NT. It does not limit space for Win95 or Win98 clients. Knowledgeable users can easily bypass Proquota. (Minas, April 99, p. 129) NT 5.0 incorporates both volume and file restrictions in its built-in disk quota manager.

NTFS does not support an "undelete" command for deleted files. In the NT file system, once data is removed from the Recycle Bin, it is gone and cannot be recovered (Strebe,1997, p. 150).

Novell File system uses its own Universal File System (UFS) that improves on FAT by caching directory entries, FAT and file blocks. Directory entries are hashed in memory for faster access. File blocks are cached and reads are reads from RAM, not disk. Writes are updated in RAM and the physical writes to disk are delayed providing reduced I/O and contention at the drive level. Turbo-FAT stores the FAT entries in RAM to reduce the time in chaining down to find the next segments when the file is too large to fit in RAM. (Nowshadi, 1994, pp. 117-120)

In the Novell file system, files are not really deleted when erased. Administrators can restore files that users delete. Deletion only occurs when administrators execute a purge. (Lawrence, 1995, pp. 483-484)

NetWare 4.0 and 5.0 have a built-in disk quota manager. NetWare 5.0 improves the file system with a new system, Novell Storage System (NSS). With NSS, larger files systems and volumes provide for more than one billion files per volume and file sizes greater than a terabyte (Drews, 1998). With NSS, mounting a 2.5 terabyte volume takes only about six seconds (Harbaugh, 1998).

3. Print Services

Both NetWare and NT provide network printing services to allow users to share printers via the network. NT provides an abstraction called the Graphics Device Interface (GDI) for software developers allowing them to write to a generic printer definition. NT, then, via the printer vendor's driver, writes to the hardware. This was a major improvement from the days when each application had to write to specific printers. In Microsoft parlance, printers are software devices, and the actual hardware printer is a print device. A print provider manages printing for a print device, spooling output if the device is busy. Print providers can also add separator pages. A number of print devices can be pooled to service the printer. (Strebe, 1997, pp. 490-498)

NetWare provides print services by capturing and redirecting print output to a network printer. NetWare uses the term print queue for the spooling or holding area for printouts. Printouts coming from the workstation are sent to the file server. NetWare has a number of queue management and print job controls. Printouts can be cancelled, paused and restarted. NetWare has a strong print job language allowing for a variety of output and scheduling options. Specific users can be designated as print operators to control queues and priorities. In NetWare 4.1 with NDS, printers are defined as NetWare objects and users can route print output to any printer object without needing to know the print queue name. (Lawrence, 1995, pp. 517 – 626)

In NT 4.0, when you select a printer, the driver is loaded dynamically (Strebe, 1997, p. 508). When printing under NetWare 4.0, you define the printer on the client machine (Boyce, 1996, p. 752). In Netware 5.0 and Novell Distributed Print Services

(NDPS), NetWare supports automated printer driver downloads and also allows the user to query printer status, capabilities and print job status (Harbaugh, 1998).

In NT 4.0, local devices can be shared among peers. Other users can use a local printer that is attached to the parallel port of a client machine. Through experience the authors have found that sharing local printers is difficult to manage and causes more problems that it solves.

Internet Printing Protocol (IPP), in NT 5.0 allows users to print across the Internet. Users can search for printers by name, capabilities and location (Microsoft, 1999, File and Print Services).

With software integrating NetWare and NT, workstations can print to either NT or NetWare printers. With the IntranetWare Client for Windows 95 or NT, a NetWare printer can be configured for Point and Print installation. A shortcut for any printer can be added to the desktop and any document can be printed by dragging the document over to the shortcut.

4. File Transfer

Providing files to other locations is an essential service. Novell has LAN Workplace file transfer protocol (FTP) as well as FTP server under NetWare NFS that is fully, Request for Comment (RFC) 959 compliant. RFC is an industry-wide adopted method of communicating and developing standards. FTP connections are made with TCP/IP and not IPX, and hence, workstation restrictions are not enforced during FTP sessions. (Sant'Angelo, 1994, pp. 632-634)

Microsoft provides FTP services in a number of ways. FTP is under the Internet Information Server (IIS) Web server and is included when IIS is installed. FTP can be

run from within the Explorer browser. Windows NT also has a command line utility. (Jennings, 1996, pp. 703-704)

5. Application Server

Since the server will be the focal point for all the clients in your network, in general you should get the fastest server possible and configure it with as much memory and disk space as possible. NT uses basically the same platform as the NT desktop to run applications. Applications or services run on the NT server just as applications run on the desktop. This facilitates application development as the platform used is the same for the NT environment. (Korzeniowski, 1996)

In NetWare, applications are integrated as part of the operating system. In most computer systems, applications run separately from the operating system. Instructions that are specific to the kernel are protected and run in a special ring zero; they cannot be run by applications. Applications call the system to execute services for the application. In this way, a bad application cannot cause the system to fail. (Lawrence, 1995, pp. 795-796; Nowshadi, 1994, pp. 79-82)

NetWare loads code to run as part of the operating system via their system of NLMs. Additional operating systems routines can be added in this way. For example, the STAT command is an NLM that can be loaded to provide statistics on CPU utilization. The MONITOR NLM can be added to monitor operating systems factors. VREPAIR NLM finds and attempts to repair disk problems. To protect against viruses, virus protection is accomplished via a VIRUS NLM. Even loading NLM's is accomplished by installing the Load NLM. (Lawrence, 1995, pp. 763-798)

Novell provided code to allow developers to build not only operating and system routine NLM's but also applications to be added into the system as an NLM. So if you had a dental application, you would write your code and combine it as part of NetWare code by incorporating it into an NLM and then the code could be loaded as part of the operating system. With this code, the Novell server could be a dedicated dental application system. NLMs provide vertical market opportunities for any application including legal, financial and medical systems. (Lawrence, 1995, pp. 795-796)

NetWare NLMs provide an environment for better performance. As part of the operating system running in executive mode in ring zero, the applications have direct access to systems resources and run faster. The design of NetWare processing is non-preemptive. Since ring zero has higher priority, no process can preempt any thread executing. Threads are time sliced rather than having a process track threads, resources, contention and interrupts. Without the need for processor intensive tracking of threads, the processing power can instead be more fully dedicated towards execution of the processes. Ring zero also is designed to provide the best performance on Intel processors. (Sant'Angelo, 1994, pp. 45-46)

Novell provides classes and books such as the Novell Press, Novell's Guide to NetWare 4.0 NLM Programming for application developers to develop code for applications to run on NetWare servers.

There are costs associated with the performance boost achieved by NLM's. First, it is difficult to write NLM's. Application developers, in a Windows environment, can write code in a variety of well-known programming languages and the code runs on the NT server. For NetWare, programmers write the application and then write an NLM

around the application to allow the code to run on a NetWare server. Therefore, developers have to go through an extra programming and debugging process for an application to run on a Novell platform. (Korzeniowski, 1996) Second, there is no protection against a poor application. Since no thread can be preempted in ring zero, a thread with an infinite loop, for example, could constantly run, taking up full cycles on its every turn. A process with a bug could crash and then also crash the Novell server with it. NetWare 4.0 provided a process for NLM's to run outside ring zero such as ring three with memory protection for testing and development. Once tested and operating reliably, the NLM could be moved to ring zero for its best performance. (Lawrence, 1995, p. 796)

If the software is a properly debugged mature application, running as an NLM has a clear advantage. Processor intensive applications, like databases, receive strong performance advantages from NetWare, and NetWare would be a preferred platform for an application server (Harbaugh, 1998).

In the NOS shootout at N+I on May 11, 1999, Drew Major said that for specific applications such as Oracle databases, Novell was still the superior, but conceded for many applications, it was simpler to use NT as the application platform. Novell is working with Intel to develop an application server running on Intel's new 64-bit Merced processor (Baltazar, 1999, p. 59).

Novell still has technology hurdles. NetWare 5.0 works using a single processor and promises symmetric multiprocessing (SMP) in the next release, still six months away in November of 1999. Novell's performance advantages are exemplified in benchmark tests. In file tests and locking, Novell produced a 380-megabit per second rate on a four way Pentium III test, far exceeding all other operating systems tested, and it used only a

single processor. Indeed in benchmark performance testing at Ziff Davis labs, NetWare using a single processor outperformed NT. NetWare handled more than 3500 requests per second running a Web server, whereas, Linux could only process 2300 transactions per second using all four processors. NT barely beat out NetWare with 3942 requests per second, but NT was using multiple processors. Although this shows Novell's performance superiority, without SMP, Novell cannot scale to larger applications. (NOS Crossroads, PC Week, May 10, 1999)

The real battle, though, is for developers. Novell has lost many developers and is having problems attracting developers to write NetWare applications. Novell may have a better platform, but despite better performance running in ring zero, without applications, Novell will not have much to run as an application server. (NOS Crossroads, PC Week, May 10, 1999)

6. Directory Services

For universal NOS addressing and scalability, there must be a robust set of directory services. NetWare 3.12 uses a flat directory listing of Novell members. With the advent of NetWare 4 series, Novell created Netware Directory Services (NDS), a hierarchical tree structure for its directory structure. NDS is compatible with the X.500 specification, and Novell is committed to the newer Light Directory Access Protocol, LDAP (Nowshadi, 1999, pp. 210-224). NDS has been out for six years and has improved through each upgrade (Byrne, 1999, p. 28). It is stable, and at the N+I Birds of Feather (BOF) discussions, NDS was identified as the leading application directory services product. Analysts, involved in building the architecture for the California State University system of 23 campuses and tens of thousands of students, cited NDS as the

only viable directory services solution. From discussions with IT managers at the Defense Accounting Service (DFAS) and the Defense Logistics Agency (DLA), the authors learned that those organizations plan to stay with Novell as they migrate to NT in order to retain NetWare's directory services capabilities.

With NT 4.0, Microsoft uses a flat file for its directories. Microsoft uses a domain model to store its list of users which is similar to the older NetWare 3 series. For NT, users in one domain can share resources without being in the second domain if a trust relationship is defined between the two domains. Trusts can be one-way, where one domain trusts the other, in Microsoft parlance, a trusting domain. Trusts can also be two-way. However, trusts for NT 4.0 are not transitive; i.e., if Domain A has a two-way trust with Domain B and Domain B has a two-way trust with Domain C, Domain A does not have a trust relationship with Domain C. Since domains must have a direct relationship, two-way trusts are not very scalable. The domain design is one of the problems with Windows NT 4.0.

However, NT 5.0 addresses many of the 4.0 problems. NT 5.0 includes the Active Directory, a hierarchical tree structure for directory services. It is similar to Novell's NDS. What Novell calls a tree, Microsoft calls a forest. The object that Novell calls an organizational unit (OU) Microsoft declares as the root of the tree. The differences occur in Microsoft's implementation. NT's directory services tools are not as powerful as NetWare's. Domains are trees and the directory consists of sets of domains. It may not be easy to move objects between trees. NT still has domains, but the domains now have transitive properties. This is typical of the iterative, slowly improved process

of Microsoft product delivery. Novell may have a better product, but Microsoft slowly, steadily improves its product along with gaining of market share.

Along with Active Directory, NT 5.0 eliminates the Windows Internet Naming Service (WINS), Microsoft's application that ties its NetBios names to TCP/IP addresses. The Active Directory will dynamically store IP addresses with NetBios names when DHCP assigns the IP address through a modification to the DNS standard, creating the Dynamic DNS. This implementation means Microsoft DNS will not be compatible with other DNS's. Also, for Active Directory to work with NT 5.0 server, all desktops have to be upgraded to NT 5.0 workstation. (NOS Crossroads, PC Week, May 10, 1999)

7. Security

Security for NT is a very large area and can be a complete subject unto itself. Although there are vulnerabilities in NetWare, because it is a network operating system that runs just on servers, it does not have the accessibility nor is it a target as NT is. NT workstation is on the desktop; it is for all practical purposes the same as NT server (except for a 10-login limitation and a few other small differences) so it is readily accessible. Even though NT has been designed with security principles such as trusted path logon with the CTRL-ALT-DEL and the security reference monitor concept, many holes and vulnerabilities have been found. Microsoft has been proactive in providing hot fixes to those vulnerabilities, but admin staff have to vigilant to install the fixes.

There are a number of defaults to be changed to make NT secure, in addition to applying service packs and hot fixes. This section covers security definitions, requirements, directions, what exists, how things are set up and what needs to be changed to make an NT environment secure – as best as we know it *now*.

a. C2

The National Computer Security Center (NCSC) defined levels of security for computing in its Rainbow Series of technical documents. Based upon DoD Directive 5200.28, subsections D.3 through D.5 and Enclosure 3 (an abbreviated version of the Yellow Book), for accreditation and security certification, government offices using unclassified business sensitive material, information processing equipment needs to be at the C2 level.

C2 is defined in the government's series of security manuals and part of the Trusted Computer System Evaluation Criteria (TCSEC) or the Orange Book. (The colors are from the color of the covers of the manuals). C2 is defined as those systems having identification and authentication, logging capabilities for auditing, object reuse rules and a system for discretionary access controls. (Russell, Deborah and Gangemim G.T, 1991, pp. 103, 156-157)

Microsoft NT 3.5 with Service Pack 3, has received C2 clearance. NT 4.0 is undergoing certification here in the United States but recently, on April 28, 1999, both NT 4.0 server and NT Workstation have received E3/F-C2 security rating in the United Kingdom. This rating is part of the Information Technology Security Evaluation Criteria (ITSEC), used in Europe and is essentially the equivalence of C2 in the United States. ITSEC Rating Confirms Security of Windows NT 4.0 (Microsoft, 1999, ITSEC Rating...).

Microsoft, however, received C2 clearance for NT in standalone mode only. NT is not C2 when it is connected to a network. NetWare is C2 for use on the network (Boyer, 1998).

Microsoft has announced its intention after the release of the Windows 2000 operating system, to undergo security evaluation under the Common Criteria, which is the new criteria that will consolidate the American TCSEC with the European ITSEC.

DoD Directive 5200.5 Communications Security requires DoD sites to have Federal Information Processing Standard, FIPS 140-1 compliant encryption. Neither Novell nor NT is FIPS 140-1 compliant. Microsoft is undergoing evaluation with its cryptographic algorithm for (FIPS) 140-1 approval.

At this point, NetWare and NT are the COTS solutions being used. The approval process for C2 and FIPS testing take a long time. While both NOSs are working their way through testing and certification, the main focus for administrators is to insure the software is configured as securely as possible.

b. Rights, Permissions, Access Lists

The basis of security in NT is in the assignment of rights and permissions. For consistency and manageability, access lists and permissions should be assigned via the use of groups. Groups can be defined with specific assignment of rights and permissions. Individuals having specific needs for access would become members of the groups having those access rights. This way, there is a partitioning of the organization into pools of access groups. It is easier to manage this set of groups than to require every user to have their own set of permissions individually assigned resulting in the need to manage all the users individually. (Berg, 1998, pp. 346-348)

Tools are available to view access control lists (ACL). Somarsoft provides a number of tools including the DumpACL, which provides a list of the ACLs for all files and folders on each NT volume. (Tittel, 1999)

c. Vulnerabilities

There are a number of Novell vulnerabilities if one can gain access to the server or the console. Basically, these include gaining access to the system by compromising the supervisor or admin account. One way is by swapping the administrative files that hold the password with the original set. This is done by changing the references in the bindery files in the server.exe program to make it think it is the initial instance. A second approach is to change the SYS volume so the server.exe believes it is the initial instance and to create a new set of bindery files which will have the blank password for supervisor. There are programs that allow you to change passwords for accounts including the administrator account. SETPWD and NTPASS are two programs where the administrative password can be reset.

The solution is to keep the server and the console secure. Use the option to lock the console in the MONITOR program. The secure console command removes DOS hacks by removing DOS components from the server memory and also prevents NLMs from being loaded from floppy. Server date and time changes are also restricted by the SECURE command, eliminating hacks using time dependent methods. By using the RCONSOLE, you can remove the keyboard and monitor from the server and access the server remotely instead. However, you will still need precautions to secure those components wherever they are and to secure the remote password. (Nowshadi, 1999, pp. 412-422)

Configuration and bugs are a source of security vulnerabilities. For security bugs, at a minimum, Service Pack 3 and hot fixes should be applied. If possible, install Service

Pack 4 but remember that SP4 includes the NT 5.0 NTFS format and is difficult to reverse if you have problems. Test in a lab for your environment first before installing.

There are many vulnerabilities and many of these are documented in the Microsoft Knowledge Base and Microsoft web site. The following highlights some NT vulnerabilities to give you an idea of how vulnerable you can be if you do not take vigilant action to secure NT.

NT defaults do not have strong password policies nor do they limit the number of times a password can be entered. Password crack programs and brute force methods can crack poor selections of passwords and the intruder can use the account that is cracked as a platform to perform insider hacking activities such as collecting passwords, use the processing power to hack more passwords or launch other attacks on other systems. Administrators need to run password checking against the Security Accounts Manager (SAM). In one test, a systems administrator using a Pentium 100 megahertz over a weekend broke 300 out of 400 passwords.

Passwords should include upper and lower case characters, a special character and be eight positions long. A seven-character password is especially vulnerable to hacking software. Specify lockout after three tries.

ScanNT is a dictionary attack on user account passwords in the SAM. This software can be obtained as a 30 day trial from the Mid Western Commerce Inc site at http://www.ntsecurity.com. L0phtCrack is a program that uses both a dictionary and then a brute force method to attack passwords from the SAM. L0phtCrack can be obtained from the L0pht site. This site contains many hacking methods and is a good site to keep up with what is going on in NT security (Tittel, 1999). A program, NTFSDOS, allows a

person who can obtain physical access to a machine to place a floppy in the drive and to boot the machine with the DOS operating system on the floppy. The NTFSDOS program gives the intruder access to files stored in NTFS and the files can be copied off the hard drive. (Nowshadi, 1999, p. 406)

There is no fix to this except to limit accessibility to the computer. Place your servers behind locked doors. Windows 2000 will have an encrypted file system (Johnston, 1998, p. 46).

NT comes with an administrator account and a guest account. The administrator account cannot be locked out and there is no limit to the number of failed login attempts. It cannot be deleted. This is a source of many attacks such as Red Button. Disable the guest account. Create separate accounts with administrative privileges for the admin and remove the capabilities of the administrator account. Note – creating new accounts does not hide the admin account. The NBTSTAT command shows activities that only admin can have and any user can determine the account name by running this command (Tittel, 1999).

Both Novell and NT provide facilities for auditing. Novell has a specific account called auditor. The auditor can review actions of the Systems Administrator as well as any objects in Novell. There is no special auditor account in NT but you can audit any NT object. You can check security logs for event types and specific activities for groups or users' file and object access that you have set to audit. Auditing can affect performance in both NetWare and NT. Many IT staffs do not turn on auditing in NetWare due to the performance impact. For NT, choose carefully what you want to audit. Try to audit for abnormal activities. Track password lockouts due to failed log on

attempts. Audit virus infections. For example you might audit password changes. Once hackers break into an account, they often change the password to lock others out. Users rarely change passwords (Tittel, 1999).

Viruses are another source of problems for networks. The well-known Melissa virus affecting e-mail has the potential to inflict large data losses and denial of service. Protect the server with virus software. DoD agencies have a license from DISA for McAfee and Symantic anti-virus software. These products will also scan the Exchange mail system and clear viruses from mail attachments. Run dynamic checking on workstations and make it a policy that the scanners cannot be disabled. Periodically run active scans on everyone on the network (Tittel, 1999).

A key to avoiding problems is to insure that you have backups. An important aspect of backing up is to test restoring. This may seem to be obvious advice, but testing backup restores is a task that is easily overlooked by busy network administrators. Stanford recently lost years of graduate work, because the backup tapes were never used until after a disaster occurred. When the hard drives failed, they discovered all the backup tapes were bad.

Backup strategies using complete backups, incremental or differential backups can be developed depending upon the amount of information and the stability or change characteristics of the data involved. An interesting test is to see how long a restore takes compared to backup time. If it takes eight hours to restore when the server fails, your management may get very antsy waiting for you to bring the system back up. NT has its own proprietary backup software, but a number of better products from Computer Associates, ArcServe and Seagate Backup Exec exist for backups.

Another component, beyond the scope of the NOS study but critical to computer security, is to develop a disaster recovery plan (DRP). Information on risk assessment, security policies and DRP can be found in most books written on computer security.

Both Microsoft and Novell provide security services. The BorderManager product provides caching, proxy, filtering and firewall capabilities for Novell. Microsoft built Point-to-Point Tunneling Protocol (PPTP) into NT 4.0, but it has to be found under the tools and options menu. In NT 5.0, it is directly in the Dial-Up Networking section. NT 5.0 also includes layer 2 tunneling or L2TP support and also virtual private network (VPN) with IPSec, a method to provide security for IP networks defined in the industry standards group's RFC 2401 and RFC 2411. Microsoft has also announced Lightweight Directory Access Protocol, LDAP support. For public key infrastructure (PKI) Microsoft is supporting Kerberos, a system for authentication and security developed at MIT in Project Athena. However this is not in any current existing version – this is a Microsoft implementation of Kerberos (Tittel, 1999).

Both Microsoft and Novell have positioned their systems for Internet access. A study from the Computer Emergency Response Team (CERT), a special team formed to handle and coordinate computer security problems located at Carnegie Mellon University, reported that the growth of incidents in unauthorized use was at 9% faster than the growth of Internet hosts. With the rapid growth of Internet, providing security has become vital. Encryption is part of the answer, and both Microsoft and Novell have VPN solutions in their product set.

Besides the Microsoft home Web page section on security, Microsoft also has a Web site called "the Microsoft Security Advisor". Microsoft TechNet and the Microsoft

Knowledge Base provide many of the configuration issues and checklists to perform. Additional resources include the Windows NT Systems Bug List. NT Bugtraq is also a recognized source of NT security problems and security holes.

8. Remote Access

Microsoft provides Remote Access Services (RAS) for remote access. Dialup networking provides connectivity from the client to other networks. NT 5.0 includes Routing and Remote Access Services (RRAS) which allows routing of traffic across a modem connection. Built in with RAS are VPN encryption and security. With the Connection Manager Administration Kit in the Windows NT Option Pack, users can set up Windows NT server to reduce remote access deployment costs with a centrally configured deployable single sign-on remote access client for direct dial and VPN (Tittel, 1999).

NetWare features a set of telephony options. A NetWare server can function as a modem server. NetWare also can combine telephone messages and fax messages into a GroupWise universal inbox. NetWare uses the Network Asynchronous Services Interface (NASI) for its remote access that can go across NetWare routers. NetWare Connect is an NLM that provides a 4.1 server to be a standalone communications server allowing up to 32 serial ports. (Nowshawdi, 1994, pp. 414-417)

9. Network Administration

Both Novell and Microsoft provide a host of graphical tools to assist in managing and administering servers and the network. Microsoft also supplies Administrative Wizards from Administrative Tools to assist in adding user accounts, managing groups,

file and folder access, adding printers, add/remove programs, installing modems and administering clients and reviewing license compliance.

NetWare 4.0 has a NetWare Administrator utility (NWADMIN) a graphical admin tool, which replaces the DOS-based SYSCON utilities of prior releases. NWADMIN works with the object-oriented properties of NDS allowing the administrator to work with the directory tree, users, printers and the containers they are in. (Lawrence, 1995, pp. 307-346)

Microsoft has consolidated a number of management tools into one Microsoft Management Console (MMC). The MMC is a common console framework for a management environment where tools or processes can be snapped into modules. For example, management of the Active Directory will include Directory Service Manager, Domain Tree Manager, Site Replication Manager and the Schema Manager. Microsoft is also featuring a Web-based Enterprise Management (WBEM) tool. (Milne, 1998)

10. Internet Access

Both Novell and Microsoft offer features designed to capture the growing Internet market. Novell has a host of applications from its own Web Server, cache, BorderManager security services and proxy. Dynamic Host Configuration Protocol (DHCP) and Domain Name Services (DNS) are built into NDS. Netware 5.0 now uses native TCP/IP. (Nowshadi, 1999, pp. 12-13)

Although Microsoft's NetBEUI protocol is fast and works well in a local environment, it is not routable. Microsoft has integrated many Internet protocols into its infrastructure environment. They include TCP/IP protocol, facilities for DHCP for dynamic assignment of TCP/IP addresses on NT workstations, DNS to translate TCP/IP

addresses and host names, WINS to relate Microsoft's NetBios names to TCP/IP addresses, Microsoft Proxy Server with network address translation (NAT) caching, and proxy and IP filtering services. (Microsoft, 1999, NT 5 Features)

A *Government Computer News* May 10, 1999, article shows a number of government agencies using Microsoft's Proxy Server for firewall use. In the survey of government organizations, Microsoft's Proxy Server was the most widely used firewall, garnering 20% of those surveyed. (Walker, 1999)

Microsoft has also integrated Internet components into its NT operating system and desktop. The Internet Information Server (IIS) web server is part of the NT 4.0 server operating system. Management of IIS uses NT's MMC. IIS includes security tied to the NT Server model and can issue and manage X.509 certificates for authentication. Microsoft provides its own browser, Internet Explorer, and the browser is integrated into the Windows 98 desktop.

Microsoft has also provided a host of Web application and development software. Each version of Microsoft Office includes more Web enabled aspects. Front page can be used to develop more sophisticated or complex Web material. Microsoft has built a number of tools for content management. They support dynamic Web pages with Active Server Pages and HTML templates, IIS Intrinsic Objects to access server variables and customized content for users, content indexing and search engines. Microsoft provides a development environment, Visual InterDev, for Web software developers. Microsoft also has E-Commerce servers for E-commerce solutions. (Microsoft, 1999, Web Services and Web Content Management Features)

Microsoft has committed much of its resources and its organization to the Internet. It has a rich and comprehensive set of products, infrastructure and security to leverage its advantages over other software development companies. Microsoft targets everyone in this arena, not just Novell but companies such as Netscape (which has now been incorporated into America Online) in the Internet market. The Internet market is very competitive, and Microsoft intends to become as successful with Internet products as they have been with application and NOS software.

D. INTEGRATION ISSUES WHEN USING BOTH NOVELL AND NT

Using and integrating both NT and Novell is a complex business requiring intimate knowledge of the intricacies of each operating system. Novell uses Netware Core Protocol (NCP) as its command language for application service requests which is incompatible with Microsoft's use of Server Message Block (SMB) protocol. Further, using both systems involve having two directories, sets of policies, profiles and access permissions. The combination of this duplication with differences, such as roaming for NT and context for NDS, along with the varying requirements and implementations from applications, makes a very complex and demanding environment for IT staff.

1. Client

As a starter you will need to incorporate both systems at login with a front end that works with both directories. Novell provides the IntranetWare client for NT. With this software, there are two tabs, one to setup logging into NetWare and one to log into NT. If the names and passwords are synchronized, you can just use one tab to log into the network and if you have successfully logged in, behind the scenes, you have been

authenticated and accepted by both NetWare and NT. If you have Exchange, NT also will authenticate you for mail services. (Nowshadi, 1999, pp. 346-350)

You also have another choice. You can use Microsoft's Client Service for NetWare (CSNW). If you have an NT environment and are adding NetWare connectivity, CSNW can be used. If you have a NetWare environment and are adding NT workstations, the IntranetWare Client is your choice. (Nowshadi, 1999, pp. 175-179)

There are two reasons to select the IntranetWare Client. It is considered a better product. The installation is smart and fairly easy. It removes any existing client including CSNW, copies its files to the System32 directory, updates the registry and adds the NWLINK protocol and binds it to the network card. There are rumors that Microsoft will be dropping CSNW in NT 5.0. Neither product works with Microsoft Active Directory although it is expected that Novell will update its product once Windows 2000 is released. (Nowshadi, 1999, pp. 173-174)

2. NIC Driver

On the network card driver, ODI may have been smaller, faster and media independent but with the practically ubiquitous Windows platform NDIS is practically a defacto standard. So Microsoft wins this battle as both NetWare and the Microsoft client use NDIS as the default. Select ODI only if NDIS is not available for your network card. (Note - Then it probably will not be on Microsoft's HCL). (Nowshadi, 1999, p. 174)

3. Directory Synchronization

With two directories, you will need to keep both in sync. There are two products to keep both the Novell directory and the Microsoft directories in sync. The NetWare Administrator for Windows NT manages the NT SAM database through NDS. NT

objects are stored in NDS. However, this just coordinates accounts. NT utilities must still be used to assign access rights. (Nowshadi, 1999, pp. 355-366)

Microsoft Directory Services Manager for NetWare (DSMN) works by copying NetWare's directory into the SAM stored on the primary domain controller. However DSMN only works with NetWare bindery and not NetWare 4.1 NDS. (Nowshadi, 1999, pp. 390-398)

Two other products are of interest when combining NetWare and NT – Microsoft Gateway Service for NetWare (GSNW) and Novell's NDS for NT. With GSNW, a Windows NT server acts as a gateway to a NetWare server. Client workstations do not need NetWare client software but can have access to NetWare facilities. The NT server runs the Gateway service, binds the NWLINK protocol and is the only connection to NetWare. GSNW translates Windows client requests in SMB protocol to NCP used by the Novell network. (Nowshadi, 1999, pp. 367-375)

NDS for NT reverses the tables on Microsoft gateway services and provides NetWare Directory Services for NT. When an application queries the Microsoft SAM database, the SAM client module sends a Remote Procedure Call (RPC) to the SAM server module. NDS for NT substitutes its code for the SAM server module and passes the application requests to the IntranetWare Client. Hence, any requests to SAM are redirected to NetWare. Clients are not aware of the substitution and think it is talking to SAM rather than NDS. NT administrative routines such as the User Manager for Domains run unmodified on a NetWare server using NDS for NT. (Nowshadi, 1999, pp. 216-224)

NDS for NT would allow more widespread use of Novell's directory services. However, rather than a goal of wider distribution and market share of the directory market, Novell has chosen to charge what could become cost prohibitive fees for a large enterprise. For each NT server, there is a $695 charge plus $26 for every client. Recall that for NT, there can be multiple domain controllers. For an enterprise of 10 sites with 1000 users, PDC and multiple BDC's for example, the cost would be $33,000 just to use NDS with NT.

4. Value

Integration of NT and Novell is possible but there are cost questions and considerations. Is all the extra work worth while? What does it gain you? Active Directory is around the corner and once it is available, it would be difficult to justify the extra cost in paying for two NOSs as well as all the efforts in keeping them working together.

E. NT IMPLEMENTATION CONSIDERATIONS

NT requires more resources than NetWare. Instead of one large Novell server on, for example, a large-scale high-end Compaq system, for 500 users, NT requires a number of servers. NT requires more memory, more disk space, more processing power and more equipment in having several servers to distribute functions such as the BDC, DHCP, WINS, DNS. You will need to factor these additional costs in when converting to NT.

Many NT idiosyncrasies can only be learned with hands-on experience. The procedures for a recent service pack are an example of this. If configuration changes are made after the service pack is installed, the service pack must be reinstalled. In general,

once a maintenance release is installed it should not need to be reinstalled when the configuration is changed.

There is no user disk space limitation with NT 4.0. Proquota, in SP4, has some abilities to limit space, but there are better disk quota products. Until NT 5.0 is available, consider some of the third party disk space quota products.

Almost everything is in the registry. Any configuration setting, change in setup, etc. are all stored in the registry. By working directly with the registry, you can set up the installation as you need. But there is a caveat here. Microsoft may not support you if you have many nonstandard registry hacks. (Russinovich, 1999)

F. KEY NT AND NETWARE DIFFERENCES

One of the main differences between Netware 4 and NT 4 is the directory and network architecture. If you move from Netware 4 NDS to NT domains, you will lose your multiple containers when you go into NT's flat structure. If you have containers with the same name but in different contexts, the names will collide in the same domain. One alternative is to set up different domains matching Netware containers. (Plumley, 1997, p. 4)

However, Microsoft, in anticipation of Active Directory Services and the steps in migration to it, has advised users to not proliferate domains and to, as much as possible flatten out the structure and to put users or domains together. The only other solution is to wait for NT 5.0 to be released.

The methods for administrative configuration management are different with NetWare and NT. NetWare has powerful login scripts. Network administrators can do a number of things by writing code. They can develop automated procedures to change

configurations, setup defaults when the user logs in and perform configuration management. NT includes login scripts but they do not have the conditional and branching capability. NT uses profiles for configuration management. Profiles in NetWare are cumulative. Profiles in NT are not – the last one entered is the one used. These are key differences, if NetWare's login scripts, group and profiles are used to manage the IT infrastructure.

Whereas with Windows 3.x and a Novell network operating system, software stored centrally on servers worked well, with NT, changes have made this more difficult. The NT model assumes that software will be installed locally. Microsoft products, even when installed from the server, write and store hundreds of megabytes of configuration files onto the hard drive of the PC locally.

The authors have experienced a number of conflicts in the products. Novell had a period where they struggled with NLM conflicts. DLL conflicts with Microsoft is an installation headache. Although Microsoft has methods to lock directories, the authors found installing even Microsoft's own software violates these restrictions.

For administrative controls, Microsoft uses Systems Management Server (SMS). SMS provides desktop management, software delivery and network management functions. These tools use different methods than comparable functions in NetWare. These tools will take some time to learn for most network administrators with a NetWare background.

G. ADDITIONAL NEW FEATURES

The major and significant new feature in Windows 2000 is the Active Directory Services. Microsoft touts the gains for Windows 2000 to include performance, ease of

administration and security. Below are a number of other features that government offices would have interest in to lower administration and TCO.

NT IntelliMirror is a highly marketed feature where the user's files, applications and systems configurations are mirrored on a server. Should the user's PC fail, a copy from the server could be copied back down to the problematic machine. IntelliMirror would also simplify roaming where users can go to any machine and have their personal configuration wherever they log into the network. Bill Gates says, " IntelliMirror combines the advantages of centralized management with the benefits of local execution, the low latency and portability and not getting into a time sharing mode where you're overloading the server infrastructure." (Johnston, 1998)

Windows Installer Service provides workstation with the ability of self-healing and is an answer for configuration management. If a user logs in and the system determines something is incorrect or has been changed, the Windows Installer Service will send the user the missing modules or incorrect DLL's and reinstall to bring the workstation back to normal. Bill Gates says, "Installer capabilities are very key because they now let you do the self-healing and just in time installation." (Johnston, 1998)

Windows 2000 will have increased security with the Kerberos model and public key encryption and an encrypted file system.

Windows 2000 will also include plug and play, support for the Universal Serial Bus and IEEE 1394 bus, and power management support for notebook computers. (Bott, 1998)

H. FINAL – MARKET SHARE COMPARISON

IT21 mandates Windows NT. Given the direction of the market, that turns out to be a good decision. If you are assigned to an organization with strong Novell loyalty, the following numbers may help change some minds about the strategy to hang on to NetWare. The market comparison data shown in Figure 3.1 and Figure 3.2 were taken from a 1998 entry on the ZD InfoBeads web site. In 1996, NetWare was clearly the leading LAN OS. In 1997, things began to change in favor of Microsoft as evidenced by the 61% of customers who were planning to install a Microsoft LAN. By 1998, Microsoft had a small lead. Figure 3.2 shows that the trend will continue, because more sites plan to convert to Microsoft's LAN OS. (ZD Market Intelligence, 1998)

LAN OS Installed Base

	Novell	Microsoft
1996	70%	16%
1997	58%	26%
1998	45%	48%

Figure 3.1. LAN OS Market Share Percentages

Planned LAN OS

	Novell	Microsoft
1996	54%	44%
1997	36%	61%
1998	25%	74%

Figure 3.2. Future Trend in LAN OS Market Share

Many believe that Novell has the better product. However, it no longer has the market share, and in the competitive IT world of today, market share means survival. There seems to be no demand for a variety of software product vendors all offering

similar products. This is due to the interoperability problems inherent in trying to use different software products for the same application. In addition, people do not want to relearn how to do something. Once they know how to use MS Word, they do not want to learn how to use another company's word processor regardless of product quality. Microsoft used their market share in the application software arena to attract customers to their LAN OS. They did this by making it very easy to integrate their applications with their NOS.

Chapter IV moves from the technical details of a NetWare to NT migration and discusses the problems inherent in managing technology-driven change and ways to address those problems.

THIS PAGE INTENTIONALLY LEFT BLANK

IV. MANAGING TECHNOLOGY-DRIVEN CHANGE

A. INTRODUCTION

"Change, in its broadest sense, is a planned or unplanned response to pressures and forces" (Jick, 1993, p. 1). Business, the military and government have dealt with change for centuries, but today's organizations are dealing with a variety of change drivers occurring at unprecedented rates. "Change is a potent issue these days, however, because simultaneous, unpredictable, and turbulent pressures have become the norm." (Jick, 1993, p.1) What is change management, and why is it important? This chapter answers those questions and looks at the importance of understanding and addressing the human factor in technological change. In recent decades, many books have been written on the art of managing change in the work place. This chapter applies several theories and practical implementation steps provided by some of those books.

Change management is concerned with all aspects of change in the workplace. Change brought on by technology advances, downsizing, realignments to improve an organization's competitive edge, new management and market demand are just a few examples of change drivers. This chapter focuses on managing information technology-driven change, in particular how to manage a transitional change like converting from NetWare to Windows NT. This discussion is directed toward operational IT managers.

Managing IT change means understanding the reasons for the change, communicating those reasons to upper and functional management, to the technicians who will implement the change (change implementers) and to workers who are impacted by the change (change recipients), and guiding everyone through the process of achieving

the intended change. It is important to understand that managing change includes managing the reactions to change. "Unfortunately, change frequently is introduced without considering its psychological effect on others in the organization—particularly those who have not been part of the decision to make the change." (Jick, 1993, p. 6)

An operational IT manager must have the support of upper management in order to successfully bring about a technology change. It seems logical that if a conversion project has been approved, then upper management is fully behind it. That is not always true. As we will see later in the case study, upper management and operational management can have different motivations for and expectations of an IT change process. In some cases, upper managers do not fully understand the reasons to invest in IT, but feel they must do so to stay in step with the times. IT managers should be clear with upper management about why the change should occur and outline what the new system will do for the organization. Make sure that upper management understands how the new technology supports what the business does and adds value. IT21 can present an interesting challenge to an IT manager, if the organization's leaders are simply "talking the IT21 talk" without fully understanding why. You are much less likely to get real support from management who does not see the real value of the new technology. Lukewarm support from upper management for a change effort equates to change resistance. Work hard to insure top management is fully aligned with the technology change you are about to implement.

You also need to solicit the support of your management peers in other departments. Include them in the planning phases of the change project. Listen to their

ideas and concerns. Open lateral communication channels are critical to the success of any project that crosses internal organizational boundaries.

Do not assume that the change recipients will be the only ones to resist the change. Your own technical workers may resist the transition to a new system. How will the technical staff, who is well versed in NetWare, feel about the mandate to convert to NT? Some will want to learn something new, because they like learning new things or want to add a new skill to their resume. Others will feel loyal to NetWare and will search out reasons why NT will not work. Therefore, you as the manager responsible for the conversion should be sure you have open communication with the project workers. They should feel free to voice their concerns regarding the conversion, and you should listen and respond to those concerns. Given that IT21 mandates the conversion to NT, many IT managers may feel they are put in the position of "defending" the decision to NetWare loyal employees. There is no simple answer to address this. Each organization has different cultures and personalities to consider. Analyzing your situation, understanding the change objective and the forces for and against the change, developing a clear plan and keeping people informed and involved will significantly improve your chances of a successful conversion from NetWare to NT.

To reiterate, communication in all directions is one of the most important things a technical manager can do to maintain a smooth change process. You need to communicate with management above you and be certain that your goals and expectations agree. Communicate with your management peers in other departments within the organization. If they are included in the planning phase of the change process, they will likely be facilitators rather than impediments to the change process. It is

important to communicate with change recipients, and it is equally important to communicate with the technicians working to implement the change. It is easy to forget that IT workers are also impacted by the changes that they bring.

This chapter discusses "Why Manage Change?" and "How to Manage Change". The "Why" section makes the case that the failure to manage change often produces disastrous results and is the reason, in part, for the IT productivity paradox. The speed of technology advancement has increased to such a rate that managing change is more critical than ever before. Information technology keeps advancing, and companies spend more and more on IT, but some believe the promised productivity increases have not occurred. Change management practices have the potential to dramatically improve the success of an IT implementation. If you do not need to be convinced that managing change is important but want some ideas on how to approach change management, skip to section C.

The "How" section provides some practical change management approaches to consider when planning a technical change. Stewart Stokes describes how to prepare for the change cycle by employing two analysis techniques. His situation analysis method is a list of questions to answer that will provide insight into the situation as it exists before the change. The force-field analysis method, developed by social psychologist Kurt Lewin, gives a framework for understanding the objective of the change and the forces working for and against a successful change implementation. Stokes' Seven-Step Process for managing change is outlined. This process addresses each step in a complete change cycle.

B. WHY MANAGE CHANGE?

The best way to answer the question, why manage change, is to talk about what happens when change is not managed or managed poorly. History provides many good examples of the consequences of poor change management. The military has always been a leading technology user. The U.S. Civil War is a good example of technological advances in warfare machinery outstripping the warfare tactics being used. The military's failure to understand and manage the changes attendant with warfare technology advances lead to the extremely high death toll in the U.S. Civil War. Early in the 20th Century, Navy leaders failed to understand the potential of air power against Naval ships. They believed that the iron ships of the day were impervious to air attack. Fortunately in this example, the military leaders quickly recognized their misunderstanding of the changes to naval security air warfare introduced.

If you do not manage change, it will manage you. Managing change is about maintaining control, which sometimes means letting your people assume control. Understanding the drivers for change and the resistance to change for a given situation gives a manager the perspective needed to identify the barriers that can delay or completely halt a technical change implementation. It is important to remember that while management must control the variables and processes that are part of the change project, employees impacted by the change often sense a loss of control. Management must involve everyone affected by the change and make them feel like part of the process rather than victims of the process.

Change management is people management. However, it goes beyond managing when things are stable. Managing people when their environment, the tools they use to produce and even their place in the organizational structure are changing is a challenge that requires leadership as well as management. Most traditional managers are skilled at managing stability, but are lost when faced with managing instability.

Today's IT managers must be even more aware and involved in change management than were their predecessors, because the velocity of change is so great and managing IT-driven change has become a critical factor in project success.

> Forty percent of IT application development projects are canceled before completion. Thirty-three percent of the remaining projects are "challenged" by cost/time overruns or changes in scope. (Field, 1997)

Why are less than one third of all IT projects completed without encountering a major snag that significantly increases the time and cost of the project? Some suggest the reasons for this dismal record are that developers fail to assess users' needs or to accurately define the project's scope, or both. Others suggest the failure of so many IT projects is that managers fail to address the issue of change. Some government and private companies have turned to risk management strategies to help improve the chance of IT project success. The State of California spent a year developing a risk-assessment model that contains five major categories of risk for large IT projects. Change management risk is one of those five categories. The state reports success with the results of using their risk-assessment model. While the typical IT project in California used to escalate in cost by an average of 85 percent, that figure has been reduced to just 15 percent since using the risk management program. (Hayes, 1998) "Research

conclusively shows that good change management skills can substantially increase the odds of IT project success." (Markus, Benjamin, 1997)

1. Velocity of Change

Many of the best-laid technical plans have been derailed by the project planner's failure to consider the human issues involved in a successful implementation of technical change. Although we live in change-driven times, people still want to feel they have control over their lives. Constant change degrades that feeling of control. When things are in a perpetual state of change, it impacts the humans that have to deal with that change. No wonder employees resist the frequent changes to their daily work routine brought on by an IT advancement.

The rate of technological change is a late 20th century phenomenon that impacts all of our lives in ways we are just beginning to understand. Each technology innovation is taking less time for the market to adopt. It took twenty-five years for the automobile to replace the carriage. It took twenty-five years for television to become a commodity. It took only twelve years for the VCR to gain widespread acceptance. Information technology products become mainstream and then obsolete at an astounding rate. Moore's Law tells us that computer processing power doubles every eighteen months. In *The Friction-Free Economy*, Dr. Ted G. Lewis refers to this eighteen-month cycle as Internet Time, and states that "the process has accelerated to the point where computer technology improves by a factor of 500 every decade!" (Lewis, 1997, p. 14) Will the rate of change within IT decrease or stop at some point? Dr. Lewis suggests that soon computing power will be bounded by the limits of human ability to absorb information and make decisions rather than by the limits of technology. Even so, unlimited access to

information, which results in learning, will continue to bring changes in the workplace and our everyday lives.

The rapid rate of IT advancement is a key reason for including change management in any technical implementation plan. The probability of a successful completion of an IT project decreases if change management is ignored. Managers need a structured methodology to help them address all of the moving parts of a project designed to introduce technical change into the social framework of an organization.

2. Critical Changes Impacting IT Managers

IT professionals have long viewed themselves as the ones who introduce change. It is ironic that the technology they were introducing began to change their roles. Over a decade ago in the 20th Anniversary Edition of *Computerworld*, Michael Hammer described the changes facing IT managers:

> This transition is not a modest one...we have embarked on a new enterprise with a new mission, new responsibilities, and new requirements...we will have to become intimately involved with the users and their businesses (this) role will demand new skills...new styles...new attitudes...(and) need to cope with a different set of pressures...(Hammer, 1987)

These words have proven to be true in the corporate world, and DoD IT professionals are waking up to the reality that their role as the centralized dispenser of information technology does not play in the networked workplace.

IT managers need to develop a stronger business orientation. In business and government, the IT director or Chief Information Officer (CIO) has moved from the operational realm of the business into the senior management arena. There has been a growing trend in the corporate world to hire CIOs with a strong business rather than

technical background. (Blodgett, 1998) Some of these CIOs have no prior IT experience. In many cases, these non-technical IT managers have outperformed their technical-based peers, because their business experience allows them to understand the business mission and align IT to support that mission. IT managers who have risen through the technical ranks often have trouble shedding their technical hats. Their background has not taught them to take the broad perspective when viewing IT and its relationship to the rest of the organization.

Increasing computer awareness and expertise among non-IT personnel is another source of pressure. While it is always helpful to have customers with enough technical expertise to serve as an interface between the non-technical customers in their unit and the IT group, there are drawbacks. Some computer savvy customers want to be given the freedom to configure their workplace computer environment. Any network administrator knows that the more non-standard setups there are to support, the more problems there are. Also, conflicts can arise when these customers, sometimes referred to as technical "wannabes," disagree with the standards and configurations established by the IT staff.

The emergence of information as a major strategic weapon is another trend that changes the traditional roles of IT management. Data centers are collapsing and the IT group is becoming another strategic business unit within the organization. Their primary function is no longer to "process data," but to provide the business with information that supports the mission and helps the organization gain strategic advantage over their competitors. An IT manager must understand the business, its environment and the competition.

Timing has always been a key to business and military success, but time is more of a competitive weapon than ever before. The group that gets out there first wins the prize. This emphasis on time increases the already high levels of stress and pressure felt by systems professionals.

IT has brought vast changes to the business community. Vice Admiral Cebrowski observed in his 1997 address at the U.S. Naval Institute that the businesses that have co-evolved their organizations and processes to exploit IT have gained tremendous competitive advantages. He believes the military can achieve a similar advantage in warfare. One of the keys to gaining this advantage is to enable "forces to organize from the bottom up--or to self-synchronize--to meet the commander's intent." (Cebrowski & Garstka, 1997) The rapid creation and dissolution of special purpose task forces lessening the impact of historical chains of command allows the flexibility needed to meet today's shortened timelines. The communication links IT provides to get information to the right people at the right time enables these self-synchronizing groups to operate. The move toward IT being the support for strategic advantage is a major change impacting DoD IT managers.

Finally, the base closings and realignments of recent years have merged people with different group cultures into one organization. The corporate world has had to deal with these same problems as organizations acquire and become acquired by other organizations. A discussion on the power of culture is included in section C of this chapter. The merging of different cultures is felt by everyone in the organization, but IT personnel must interface with virtually every group. Management guru, Tom Peters says,

> I believe that the real legacy systems that have to be changed are those that involve the corporate culture. I can learn more from studying Gandhi, King and other community and social activists than I can from going to another meeting of geeks." (Peters, 1998)

As we will discuss, understanding and working with the organization's culture and subcultures is a requirement for the successful IT professional.

3. Productivity Paradox

Most people agree that computers have the potential to allow us to lead simpler and better lives. Those same people would likely agree that so far computers have not lived up to their promise.

> The common notion today is that computer technology will swiftly lead to vast improvements in productivity. But despite the fact that computers are everywhere in our lives, we have a lingering doubt. Innovations with computers have yet to translate into recognizable impact to our overall productivity. This quandary has been termed the "Productivity Paradox." (Craine, 1998)

Much has been written about the IT productivity paradox. Organizations have spent millions and even billions of dollars on their IT infrastructure and many of those organizations report that they have yet to see an appreciable return on their IT investment. Is there a productivity paradox? It depends. If traditional productivity measures like return on investment are used, the answer seems to be yes. If intangible benefits like the ability to provide better customer service are considered, the answer may well be no. Whatever the answer, IT has not yet truly made our daily lives easier.

Michael Dertouzos, Director of MIT's Laboratory for Computer Science, bemoans the fact that computer technology has not yet lived up to its great promise. It is easier to talk about how computers can be used to improve productivity than it is to implement an

effective IT system. "I see ridiculous duplication of effort. People are doing everything they used to do before computers plus the added work required to keep computers happy or to make people appear modern." Dr. Dertouzos sees both technology and the misuse of technology as causes of the productivity paradox. (Dertouzos, 1997)

The major reason for misuse of technology is that organizations do not spend the time analyzing what their core business is and how computers can help improve their ability to conduct that business. An organization's failure to analyze how the technology aligns with its business mission is ultimately a failure to manage change. Too many IT procurements have occurred simply to appear to stay in step with the times and the competition. IT managers first must understand the organization's business and the environment in which it operates before they can implement IT as a tool to enhance productivity. The organizations that invested a lot of money in IT and believe they have seen minimal or even no return on that investment need to re-evaluate their IT acquisition justification. They need to adopt a change management methodology to help them analyze when and if a technical change should be implemented.

4. Magic Bullet Thinking

Managers need to stop looking at IT as a cure-all. Managers want so badly to believe that there is something out there they can simply purchase that will solve all of their problems, and IT marketing targets that unrealistic expectation. In a 1997 *ComputerWorld* article, M. Lynne Markus and Robert I. Benjamin warn IT managers against "magic bullet" thinking. They say that best practices in change management are not widely used by IT specialists and line managers due to their belief in an IT magic bullet.

> Successful organizational change is a contact sport. Change is not produced by planners planning, designers designing and funders funding. Rather, it is the result of hard, interpersonal work by all the actors in the change drama, where the tactics can range from infinite patience to the use of metaphorical two-by-fours. The magic bullet theory's seductive appeal is that it will do the hard, contact sport work for all of those who prefer disembodied ideas to "in-your-face" contact with the users who are targets of change. (Markus and Benjamin, 1997)

Business administration professors, Anandhi Bharadwaj and Benn R. Konsynski, of Atlanta's Emory University write, " Even when IT benefits accrue, it can be difficult to separate out IT's contributions because improved results are typically achieved by pairing IT's benefits with supporting investments in such programs as reengineering and total quality management." (Bharadwaj, Konsynski, 1997)

Even with all of the challenges IT brings, it has also brought major improvements to many processes. Michael Dertouzos reminds us that, "we are only thirty years into the new technologies of information. It took more than a century to move the world from steam engine to internal combustion engine. Some patience with this young field is in order." (Dertouzos, 1997)

5. Summary of "Why"

Change always has and always will be a fact of life. The velocity of change has increased in the late 20th Century and nowhere is change more rapid than in the IT field. The poor success record of IT projects and unrealized computer-generated productivity gains tells us that something is missing in the IT implementation formula. The missing component is change management. Organizations that have changed their implementation plans to include change management have seen a significant improvement in their IT project success rate. Change management is not an easy "magic

bullet" to cure all that ails the IT manager, but it is the missing element that when included throughout the life cycle of every IT implementation will significantly increase the odds of the project's success.

C. HOW TO MANAGE CHANGE

The first step in the process is understanding that change must be managed. This section addresses the question of how an IT manager incorporates change management into a technical implementation? Stewart Stokes advises that, "Every change comes complete with its own special circumstances; the more you consider these situational variables, the easier it will be to introduce and manage the change." (Stokes, 1991) Stokes' Seven-Step Change process is a change implementation model for middle and lower IT managers who must introduce and manage change on tactical and operational levels.

1. Getting Started

Before you can develop a change implementation plan, you must understand your organization's unique environment. The following is a list of questions to help you begin to see the challenges your particular environment presents. This list was adapted from two methods--Situation Analysis and Force-Field Analysis. These questions can help IT managers analyze the change implementation process. The Situation Analysis questions are designed to help you to understand the variables that impact the change process in your organization. They help you understand your and others' perceptions about the impending change. In addition to the Situation Analysis method, Stokes recommends a process pioneered by social psychologist Kurt Lewin called Force-Field Analysis. This identifies the forces in your environment that will work for and against the change you

plan to implement. Situation Analysis and Force-Field Analysis overlap somewhat. Therefore, the following list of ten questions merges the two methods. The answers you find for these questions will be used as you begin the Seven-Step Change cycle.

Figure 4.1 provides a quick look at the list of questions. A discussion of each question follows.

1. **What forces are driving the change?**
2. **Is there a well-stated goal of where the change will take the organization, and do all of the stakeholders understand the goal?**
3. **Who is impacted by the change?**
4. **Who is likely to resist the change?**
5. **Can you do anything to minimize the resistance?**
6. **Who is likely to support the change?**
7. **Can you do anything to maximize the support?**
8. **What is the organization's history of change?**
9. **What is the organization's culture, and how will it impact the technology implementation plan?**
10. **Does the organization's structure support or inhibit change?**

Figure 4.1 Situation and Force-Field Analysis Questions

What forces are driving the change?

Understanding the reason or reasons for the change is crucial. There are people and environmental factors behind every change effort. Without a clear picture of why the change is occurring, you cannot develop a successful implementation plan.

Is there a well-stated goal of where the change will take the organization, and do all of the stakeholders understand the goal?

If you do not know why the change is happening and the good it will do, you cannot effectively "sell" the project to potential supporters. Be able to clearly articulate why the change is a good thing for the organization. Do not simply use the tired old reason, "It is mandated by ...".

Make sure everyone understands why the change is occurring. Make it a priority to educate all of the people impacted by the change and do it early in the process. Be proactive. Do not wait for people to come to you and ask why or oppose the process because they do not understand the drivers and the benefits of the change.

Who is impacted by the change?

In a sense, everyone in an organization is to some degree impacted by a technology change. It is reasonable to try to identify how each part of the organization will be impacted, but it is crucial to consider how the people whose daily work will be altered by the change will react.

Who is likely to resist the change?

Once you know why the change is occurring and who will be impacted, this is the most important question to ask. It is a given that some people will work against the plan to implement change. You must identify them and try to understand the reasons for their resistance. People resist change for many reasons. Most of us like a routine, because it gives us a sense of control. Resistance is often a reaction to a perceived loss of control rather than a direct resistance to the change itself. There will often be other forces that want to maintain the status quo. Some people will feel that moving to a new system is a condemnation of their previous decisions and actions. Organizational politics, people with special interests in the old system, formal and informal organizational structure, organizational culture and just plain human nature are all potential roadblocks to change.

Can you do anything to minimize the resistance?

If you understand the reasons for the resistance, you can often eliminate it. Involving the people who will be most directly impacted by the change in the early stages

of the planning process is one way to reduce resistance.

Who is likely to support the change?

In addition to the people who are actively driving the change, there will be others who will support the change effort. Find as many of these people as you can. It is best to find them at all levels of the organization. Upper-management support is required for any change effort to be introduced, but involving people at the operational level is just as critical to the overall success of the change implementation. After all, the people at the operational level will be most directly impacted by a technology change.

Can you do anything to maximize the support?

Once you have identified people who will support the change effort, involve them in the planning effort. You want the supporters to feel ownership in the change project. These people can then be ambassadors for the change in their various parts of the organization.

What is the organization's history of change?

This question is not limited to technology change. It addresses all types of change, organizational structure, mergers, downsizing, acquisition of new areas of responsibility, and others. Anything that has changed the work environment should be considered. The DoD has always dealt with a changing world, but individual groups within the DoD may have enjoyed relative stability for many years. The end of the Cold War and the subsequent budget cuts of recent years have left very few DoD organizations untouched by change. If your organization is one where major changes are ongoing, you have to be especially careful in your approach to changing a well-known technology.

> There are limits to the stress that organizations can absorb--either at a given moment or cumulatively. Organizations, like individuals, can become saturated, and, thereby, be either unwilling or unable to integrate new and deeper changes, even if these are acknowledged to be needed. (Jick, 1993, p. 7)

What is the organization's culture, and how will it impact the technology implementation plan?

"Culture is the repository of knowledge and values that guide behavioral decisions related to performance." (Pasmore, 1988) Deal and Kennedy succinctly define culture as "the way we do things around here." (Deal, Kennedy, 1982) The term culture covers everything from the way employees dress to how they deal with each other and their customer to provide the organization's products or services. "When the cultures are our own, they often go unnoticed--until we try to implement a new strategy or program which is incompatible with their central norms and values. Then we observe, first hand, the power of culture." (Kotter & Heskett, 1992)

An IT manager needs to recognize the cultural "rules" and work with them not against them. This is particularly true when you are planning to introduce a technical change. The DMDC case study in Chapter V describes how the Systems Department's attempt to "lock-down" the desktop for network stability violated the network-users' belief that the workstation on their desk is their tool to configure and use as they see fit. DMDC's culture rewards the people who can provide quick results. The DMDC network customers felt that if you had to call Systems every time you needed to do something outside of the standard configuration, your productivity would suffer. As you will see, the "battle" between Systems and their customers significantly impacted the NetWare to NT conversion project at DMDC.

Keep in mind that there is often more than one culture within an organization. Large organizations and even some small ones usually have sub-cultures. Each functional group has its own rules and identity formed by the requirements of the work they do. For example, many IT shops have a less restrictive dress code than the rest of the organization, because many of their workers are required to crawl under desks to repair a network or workstation component. Their workday hours may differ from the organization's norm, because network maintenance and testing must be done after hours. In some organizations, the functional cultures may be as strong or stronger than the corporate cultures. You must have an awareness of the cultural norms of your organization and each of the functional groups that will be impacted by the technology change. Does the new system change any of the cultural rules? If so, involving the recipients of the change in the early planning stages is even more critical. Build an environment of teamwork rather than an "us and them" situation. The attitude of, "We're here to upgrade your system. Get out of our way." rarely builds cooperation.

Does the organization's structure support or inhibit change?

Organizational structure is the formal organizational framework which defines authority and decision making powers. It defines the ways employees communicate, work responsibilities and organizational roles. "When it works, people understand what is expected of them and how to best cooperate with others. When it fails, there is conflict and confusion about authority and responsibility..." (Jansen, 1984) So the question really may be, does the organization's structure work? Symptoms of a structure that is not working are: conflict and confusion about who has the authority to make decisions, information is not communicated to those who need it to do their work, and a lack of

coordination between work groups and departments. It makes sense to reorganize, if the structure does not work. Unfortunately, at many DoD sites reorganizations are akin to shuffling papers on a desk. The piles are stacked and rearranged but are not organized into a structure that makes frequent reorganizations unnecessary.

Even when the structure does work, the traditional hierarchical structure used by most DoD sites often lacks the flexibility to implement organization-wide changes as quickly as flatter more decentralized structures. This is due to the limitations of vertical communication channels inherent in the hierarchical structure. It takes time to go up and back down the chain when an action crosses functional boundaries. One approach for a project like a networking upgrade that impacts all functional areas of the organization is to build a team comprising members from each functional area. If the team is supported by upper management and manned with the appropriate personnel, it can serve to open communication channels that would facilitate cross-functional change. Self-synchronizing work groups advocated by those with the network-centric view would have the ability to form, open appropriate communication channels and accomplish the change. The group would disband when the project is completed, and a new group of the same or different people would form for the next project. The key for this to work is that each member of the group has the authority to do what needs to be done.

2. Seven-Step Change Process

After you begin to understand your unique environment, can clearly state why the change is taking place and have identified the forces that will resist and support the intended implementation, you are ready to use the Seven-Step Change model to begin your change process.

The seven steps represent an entire change cycle. Figure 4.2 diagrams the process developed by Stokes. The following is a summary of each step.

Step 1: External and internal pressures to change are exerted upon the organization or enterprise and the people within it. Opportunities and threats are present in both external and internal pressures. These opportunities and threats impact both individuals and organizational units. If you identify and understand all of the opportunities and threats associated with the change, that knowledge will prepare you to respond to change resistance.

Step 2: A vision for a future state is created. This may be a brief statement or an in-depth scenario. It may contain a new and/or revised mission statement, as well as broad goals and/or more specific objectives. As discussed previously, this is where you identify what the change will do for the organization.

Step 3: Benefits of the change for people and for the organization are developed and made explicit. These benefits will need to be communicated early. The clearer and more specific the benefits, the better. This step is similar to Step 2, but it emphasizes the benefits specific to groups and individuals. If this is done well, the level of change resistance can be greatly reduced.

Step 4: This step departs from the Stokes model. He lists fifteen key variables that will impact the change process. Those variables are covered in the "Getting Started" with these exceptions:

1. How much time is available to implement the change?
2. Are there training, education, and coaching resources available? To what extent?

As you will see in the DMDC case study, allowing enough time to complete the project is vital. It is often difficult to accurately predict the timeline, and many managers fall prey to the desire to deliver only good news. They report that the project can be completed in a much shorter time than is realistically possible.

Identifying training resources early is important. If you plan to provide "just in time" training, you need to be sure that the resources will be available when you need them.

Step 5: Reasons for resistance to the impending change are determined and ways to deal with the resistance are planned. You identified likely areas and individuals where resistance would arise, and you began to determine ways to minimize that resistance. This step is where you finalize your plan to deal with resistance to change. Remember the opportunities you identified in Step 1 and the benefits you found in Step 2.

Step 6: Strategies for introducing and managing the change are designed and implemented. These will range from highly directive to less directive and will include varying degrees of participation. Your strategy will depend on the organization's culture, the timeline and the available resources.

Step 7: Post-change follow-up, reinforcement, and support will help solidify the change and prepare people for further, on-going changes. This is an important step, and one that is easy to forget. Once a project is declared complete, the temptation is to move on to other things. If you take the time to review the change and how it has impacted the operational departments you will learn how to improve the next change effort. Asking customers for feedback on what worked and what needs improvement will show them that the IT group is committed to providing a service that meets the needs of the

employees and the organization. When it comes time to implement the text technology change, you will likely find less resistance and more support, if you do a good job on follow-up.

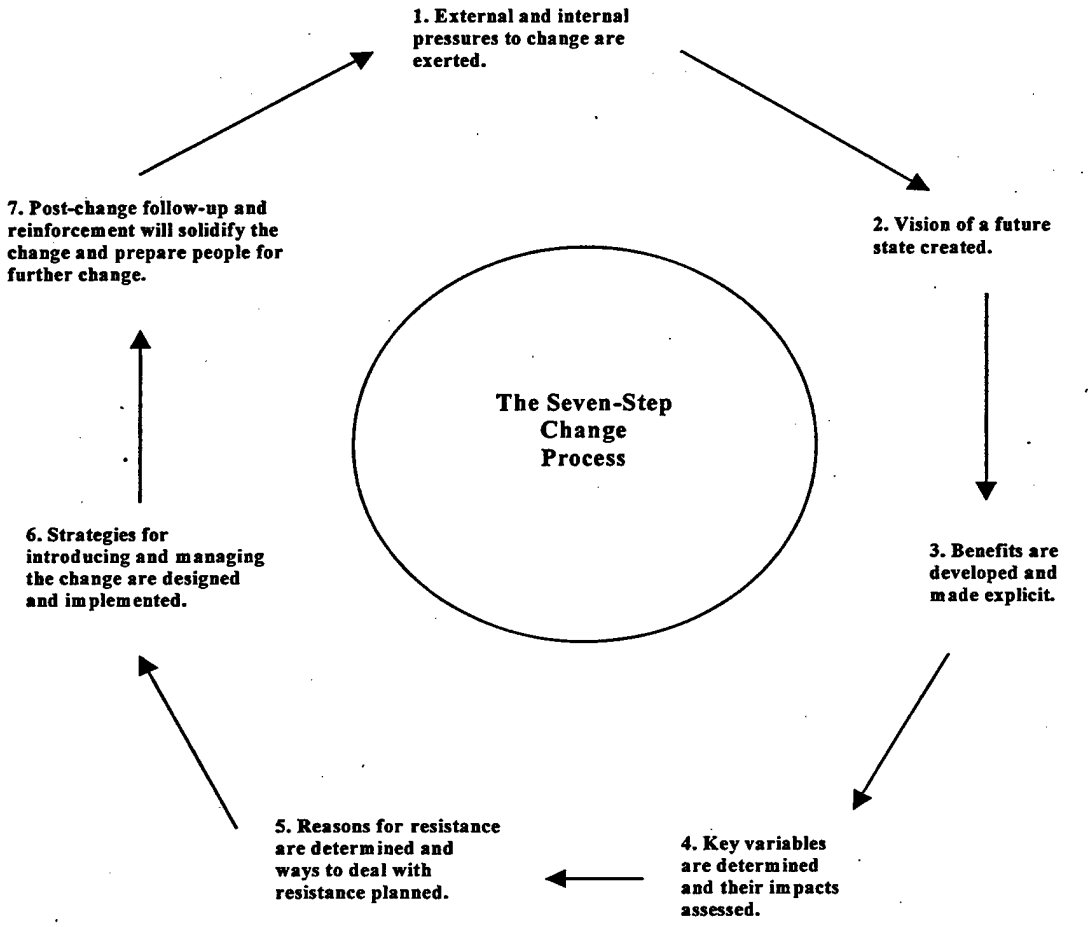

1. External and internal pressures to change are exerted.
2. Vision of a future state created.
3. Benefits are developed and made explicit.
4. Key variables are determined and their impacts assessed.
5. Reasons for resistance are determined and ways to deal with resistance planned.
6. Strategies for introducing and managing the change are designed and implemented.
7. Post-change follow-up and reinforcement will solidify the change and prepare people for further change.
The Seven-Step Change Process

Figure 4.2 The complete Seven-Step Change Process (Stokes, 1991)

3. Summary of "How"

It is clear that managing change is a complex process with different pitfalls and challenges for each unique environment. You must approach the change process using some means of organizing all of the "moving parts" of the project. The situation and force-field analysis questions help guide your thoughts to areas that present challenges to your change effort. The information you gather in that beginning phase will be used in several stages of the change cycle. The Seven-Step Change Process models the steps involved in the introduction of technology-driven change. It gives you a framework for understanding, planning, implementing and reviewing a technology change.

V. NETWARE TO NT CONVERSION AT DMDC: A CASE HISTORY

This chapter describes the migration from NetWare to NT at the Defense Manpower Data Center. The DMDC case provides a "real life" perspective for the theory and concepts from previous chapters. Chapter VI presents an analysis of the case.

A. THE ORGANIZATION: DEFENSE MANPOWER DATA CENTER (DMDC)

DMDC is the DoD's archive on manpower, personnel, training, medical eligibility and financial data for anyone who has served in the military on active duty or reserve or has been employed as a DoD civilian. DMDC's primary mission is to collect and process military and civilian personnel data. DMDC collects information from and works with the military services, DoD agencies, Health Affairs, Reserve Affairs, Office of Personnel Management, Veterans Administration and other government entities. DMDC reports to the Office of the Under Secretary of Defense for Personnel and Readiness (OUSD/P&R) and the Under Secretary of Defense for P&R. DMDC provides the personnel information required by Pentagon decision makers.

DMDC prides itself on being a "can do" organization, and its staff works many extra hours to complete "impossible" missions. DMDC quickly fulfilled President Clinton's executive order to provide the delinquent parent database. DMDC collected Persian Gulf disease data and sent letters to thousands of service members who may have been afflicted. DMDC worked financial fraud and abuse and sent technical staff with Defense Finance Accounting Service (DFAS) auditors into the steaming Philippine jungle to audit and verify continued eligibility of retiree annuitants.

Information technology has been a key component of DMDC's success. These include a broad range from database, client server and Web to data mining, artificial intelligence, rule-based and biometrics fingerprint and facial recognition technologies. DMDC has worked globally with its British and Australian Defense counterparts. DMDC technicians have flown to South Korea to install fingerprint and biometrics technology using wireless networks and to Thailand to participate in military exercises on Smart Card technology.

DMDC is located in multiple offices in the Washington, D.C. area and in a facility in Monterey, California. The Systems Branch, located in Monterey, supports the 1,000 workstations installed at the multiple sites. Although functional activities occur throughout the various sites, the California office is the technical center of the organization. There are over 400 desktop computers in the Monterey office. This case focuses on the California facility's NetWare to NT migration.

B. NT 4.0 AT DMDC

1. NT Business Drivers

DMDC needed to move to a 32-bit computing environment to utilize the advances and capabilities of new hardware and software. DMDC's primary customer, P&R, upgraded to Microsoft's 32-bit version of Office. In order to maintain compatibility with P&R's documents and spreadsheets, DMDC had to follow suit. In addition, DMDC developers required a 32-bit environment to build multi-threaded client server applications with Oracle for the Defense Eligibility Enrollment Reporting System project.

Novell's strategic direction also drove the change to NT. Novell gave up the application market. Although Novell continued to support existing application servers, it

dropped using the operating system as an application platform. This forced DMDC to use NT servers.

2. The Plan

Although NT appeared to be the logical answer for DMDC, there was little NT expertise available. DMDC Systems network expertise was in TCP/IP and NetWare. Systems decided to continue to use NetWare and ease into NT. At the time, there was little NT expertise anywhere. A complete switch to NT presented substantial risk, given the limited NT experience. To reduce this risk, Systems decided to transition to NT. The existing Novell infrastructure would continue to operate, and NT would be combined where needed with NetWare. Over time, the staff would gain experience and expertise in NT. This seemed the most reasonable process, and it provided flexibility. NT seemed to be gaining market share, but Novell was still very strong. NT was still new, and it was not clear what the future would hold. If the market and products dictated NT as the NOS, DMDC could phase out Novell.

A plan for resource and training requirements was needed to begin to implement NT. DMDC had one Compaq server to handle over 400 users with NetWare. DMDC used four servers to provide the infrastructure to support NT services. NT required more memory and more disk space than Windows 3.11. New Pentium workstations had to be purchased to replace 486 machines. A project plan was developed after a number of engineering sessions. A presentation with slides and charts was made to the Deputy Director. Project completion was estimated to be six months after the new equipment arrived. This project plan was approved. This information was shared with the staff in a series of technology direction newsletters in September 1997.

3. What Happened

DMDC was too early in adopting NT. Much of the information about an NT bandwagon turned out to be strictly marketing and press releases. The Systems staff was surprised at how little support NT had from vendors. In December, approximately the half way point in the time estimated to bring up an NT server, Systems still could not get drivers for its Intel network interface cards (NIC's). The Intel card was the DMDC standard and was used on all of its desktops. Without the driver, NT could not be installed on the network. This was a surprise: Intel was a partner in the WINTEL (Windows and Intel) consortium, but they did not have network card drivers to support NT.

The project could not be completed within the estimated six months. The estimate was too ambitious for a large-scale project given the uncertainties of a very new operating system. There were technical complexities as well as personnel problems. Incorporating NT with Novell proved much more difficult than expected. It was particularly difficult because of the animosity and competition between the two companies. Microsoft would not support Novell products and had versions of its own. It created NWLINK, its own version of Novell's IPX.SPX protocols. As explained in Chapter III, two products, one from Microsoft and one from Novell, were needed to coordinate logging onto the network.

Many of the technology decisions Microsoft made seemed based upon competition and marketing. For example, Microsoft had no directory services similar to the X.500 standard. In sessions on Novell integration at Microsoft conferences, Microsoft announced support only for the older Novell bindery. Microsoft would not

support Novell's directory service. Microsoft provided a migration tool to move users from NetWare to NT, but provided little to make it easy to integrate the two products. Microsoft asked some of their largest customer accounts to promote a total NT solution. Australian Telecom (AT), a Microsoft customer running 16,000 workstations and many Novell servers, advised users to replace NetWare with NT. AT said the size of their network should resolve any question people might have on NT's scalability. US Trucking, another large NT customer, advised users to drop Novell.

Systems encountered countless technical problems in the NT implementation. A lot of time was spent trying to figure out why the Microsoft policies would work only intermittently. The implementation of a policy is a key part of setting up controls. The team was perplexed and worked on this for weeks only to find out that it was a bug in the Novell 32-bit Workstation Manager. This product coordinates the Novell and NT logins when users first log in the network. As explained in Chapter III, this was a more flexible product and supposedly better than the Microsoft version. No one could figure out why and how it affected NT policy but it was a documented problem. Loading the patch resolved the problem.

Much of DMDC's design and controls were based around login scripts. NetWare and NT login scripts operate differently. DMDC used the combination of login scripts and network groups to control users' access to network resources. As previously mentioned in Chapter III, NT login scripts are weak. They do not have conditional and branching capabilities. NT policies are not cumulative and do not work the same as NetWare's policies. NetWare allows multiple policies and the results are cumulative. In NT, the last policy overlays all previous ones.

DMDC had expertise in Novell and had used the strengths of Novell in managing and deploying its network and strategies. NT was different and the Systems staff had difficulties in trying to make it do what Novell could do. At one point, Systems management finally said, "We think Novell. We have to stop thinking Novell and think NT."

Although Microsoft advertised NT's capabilities for strong administrative control, in reality, NT did not provide adequate control. NetWare provided strong access and permissions control on the server, but the controls on the desktop with Windows 3.11 at DMDC were mainly administrative and through directives. There were few technology tools to control the desktops. DMDC policy stated that no software could be brought in from home or downloaded from the Internet to be installed on a DMDC workstation. All software was to be stored and retrieved from the servers. But there was little to stop users if they loaded software. If the incident was particularly blatant or egregious, there could be employee disciplinary action. However, Systems did not want to be in a PC police, enforcement role. The only tool employed by Systems to convince users was to give priority on support to users who had problems with the standard system. Users with nonstandard, modified setups received lower priority in receiving help from Systems technicians. When Systems encountered transgressions (generally when people had problems) the only recourse was to format their computer and reconfigure it to the standard.

Systems looked forward to NT, which supposedly would provide the technical mechanisms to lock down the desktops. A lot of effort went into this, and it turned out to be quite elusive. Yes, directories could be locked down, but then applications would not

work. For example, the idea was to protect NT on the desktop so the user could not mistakenly wipe it out. This was not doable. NT was loaded into a separate disk partition on its own and access by the user was limited. But applications owned by the user needed to write into these directories. For example, Win32 and WinNT directories were originally locked and then had to be reopened. The organization chart program in Microsoft Office wrote to these directories.

Microsoft had a controlled desktop configuration under an initiative called Zero Administration for Windows (ZAW). Microsoft introduced ZAW to compete with the emerging network computer concept, and advertised that it would reduce total cost of ownership (TCO). When DMDC Systems considered implementing ZAW, they found it was not a product, but rather a concept. Microsoft provided an assortment of tools to help the user implement ZAW. However, it was inaccurate for ZAW to be advertised as a fully developed product that could be easily integrated into an NT system. The zero administration tools are provided in the NT systems development kit (SDK) and are referred to as the Zero Administration Kit (ZAK).

These technology limitations were further exacerbated by differences in philosophy among some of the new personnel who were hired for their NT experience. Behind the scenes, the DMDC method and standards were questioned as well as all the work and the need to manage the desktops. The new personnel felt that users were not stupid and, instead of sheltering them, they needed to take an active role in learning the technology. NT could be installed out of the box, and users could configure their desktops any way they liked. Instead of installing software on the server, users could install it on their desktops themselves with CD ROM's.

The goal was to have three working models of the new configuration ready at the half way point. With the difficulties in obtaining drivers and other technical issues, along with crosscurrents in direction, progress became limited. There were no workstations ready, and the milestone was missed. Eventually the team dynamics resulted in reorganizing the team with new leadership. The six-month projection was missed. However, the rollout of the 32-bit applications elsewhere at DMDC client sites was also delayed as developers were also experiencing problems. With the complications that occurred, DMDC management sat down with Systems and the new team and gave the project an additional six months.

4. Inherited Problems

The reorganized team accomplished several objectives. The team worked out the combination of Novell software served from the Novell file server and NT authentication, accounts and domains in preparation for Exchange. WinInstall was used for software installation. Image cast software allowed the Systems Department to clone configurations which was an important step in being able to deploy NT to over 400 machines. Without a cloning program, the installations would have to be done manually resulting in a process that would have taken much longer. However to get the new configuration accomplished, an inordinate amount of registry hacks had to be done.

Three sample machines were set up for users to try out. An early adopter program was established. The configuration was available with a caveat that it was a production/test configuration. Those who felt they needed NT immediately could sign up as an early Adopter. This program accomplished two objectives. First, it included change management components: working with the staff, allowing them to participate in

the technical change, providing Systems with feedback and developing user buy-in. Second, it acted as a pressure valve for those who had been pressing for NT as an urgent requirement. Machines were also setup temporarily to act as file converters to take care of the documents that were coming from Pentagon staff in the new format.

As the team closed in on deployment, two new problems emerged. First, the developers balked at the administrative controls. As described above, compliance was not actively monitored, allowing the developers to believe they were free to do the things they needed to get their job done. As NT came closer to reality, the programmers were aware that local admin privileges would not be granted, and they could not modify their machines.

This problem was resolved at two levels. Systems worked faster and was better prepared with facts and information in a showdown meeting with the Deputy Director. Systems won management backing for their plan. But even with management support, by working closely with the programming supervisors, much of the rancor was eased. The key senior programmer agreed with Systems that he would, himself, be nervous in granting change privileges to some of the programmers. The supervisors offered to regulate themselves and to control the change capabilities through only the supervisors. This was accepted by Systems.

The second problem was much more pervasive and extensively slowed the migration. In converting machines to NT, all the past "sins" began to be uncovered. Recall that Systems did not want to be in the role of PC police. People had games, little favorite utility programs, software from the Internet, personal screen savers, etc. All were now not only exposed but some users wanted them installed on their new machine. It

was a once in a lifetime (actually in IT terms, one of many PC lifetimes with each major upgrade) opportunity to clean up. But it took a long time to sort out products and to insure licenses covered these newly discovered products. It took time to get management approval for the products. It then took time to figure out how to load the software from the server and how to do the WinInstall and the image cast. The inherited problems from the previous machine were now visited upon the new machine. This was a major holdup in completing migration and having engineered solutions for deployment. The decision from management in the one-week ultimatum was to not wait for the sanctioning and engineering of this new raft of special software. This software would be suspended for management review later. NT needed to move on with the strategic product set and what management considered to be the authorized list of software.

5. Implementation Procedures

Implementation was planned in several component parts. There was a change management component, a training component and a deployment.

From the change management perspective, Systems prepared users regarding the need for the change to NT, and then provided several machines for users to try out in the test lab. The Early Adopter program (see Attachment 1) also allayed fears and let users have the opportunity to try the configurations and provide feedback and get buy-in on the program.

The training program proved to be another problem area. Early on, the DMDC trainer tried to work with the Systems staff on what should be covered for training. The DMDC trainer had gone through an NT desktop training class. Since Systems locked down the desktop, the trainer wanted to know what it would be like and what users could

do or not do. Systems met briefly with the trainer but was too busy to provide a detailed review of the new system. Also, the design was too much in a state of flux to really know what the trainer could present. However, the trainer had to have the training materials printed and in the absence of any more information on the deadline date, went ahead and had the material printed. This turned out to be embarrassing later when the trainer taught users to make changes only to find out they were "grayed out" and unchangeable on the desktop machines that were delivered. For example, users were told that NT machines required 64 megabyte-memory, and this was in conflict with the management edict that NT 4.0 machines with 32 megabyte-memory were functional. Management refused to fund the memory upgrades. A saving grace was that few people attended the training. So one problem counterbalanced the other.

The deployment was done in several phases and the rollout process took many weekends. The first phase involved detailed planning and coordination with the users. At the outset, Systems management contacted each Division Chief and went over equipment, configurations, and requirements in general along with the deployment schedule with them. Each division had two technical representatives. These representatives were a liaison from the divisions with Systems to bring up issues, problems and concerns and to take back to their division Systems changes, directions and plans. The representatives provided backup on data for each division. Systems held meetings with the technical representatives and explained the design and the plans for rollout. The role of the tech representatives would be to work with the users to insure their information and data were saved prior to migration and also to work with users after the turnover to insure the user was up and functioning.

There were three categories of DMDC software licenses. The first category was software that was licensed for everyone at DMDC and was the core standard system. Software in this category was Microsoft Mail, Microsoft Office, Rumba, a mainframe connectivity and 3270 emulation package and SQL*Net, for Oracle connectivity. A second category was software that was older and no longer fully supported but was still required by the user. This software was at the end of its life cycle. No upgrades would be procured for this software and hopefully, over time, this software would be phased out. Examples of this software are Lotus 123, Word Perfect, Harvard Graphics and Freelance. The third category consisted of unique software needed by the users. This software was current software but with limited licensing for those who needed the software. Examples of this category were SAS, SPSS and Procomm communications software.

In the preparation phase each user's configuration was reviewed and a list of the user's new setup was organized and prepared in advance. For each user a data sheet was compiled to document the user's configuration.

In the rollout phase, supervisors were notified each week which users would be migrated to NT. Systems worked with the technical representatives to insure all of the user's information and data was back-upped just before the switchover. Each user was to move the data they needed in the new system into one directory called Mydata. The data could be organized into subdirectories under Mydata. The technical representative visited each user and worked with the users. They showed users how data could be copied by dragging them into the directory if the space was available or just moved into the directory if space was limited. DMDC had standards for storage of data. For example mainframe data was generally kept in MFDATA; Word documents were stored in

WORDDATA; PowerPoint in PPDATA and Excel in XLSDATA. The technical representative also interviewed the user regarding important projects to make sure data were not stored elsewhere and would be missed. The representative did a final review of the disk directories and then made backups on ZIP cartridges before the final shut down.

The new machines were set up with the NetBIOS name and pre-installed with the DMDC standard software prior to the weekend. Each users configuration and equipment was identified and labeled with the user's data sheet. Any additional software in the second or third software category was installed. Depending upon where the user was located, different printers were installed and the standard printer for that floor was set as the default.

On Saturday morning, the Systems team did an unadvertised network backup of the user's computer. This data would be eventually moved to tape. A second team collected the machines. The computers were kept aside for a week as a third level of contingency planning should there be misunderstanding and something important was overlooked and left on the computer. The new machine was carried to the user's desktop and connected to the network. A quality assurance (QA) team made up a third weekend crew. Logging into the machine as a local admin, the QA team checked each machine setup from the network connection to insure the installation matched the data sheet and the applications worked. Finally, a pamphlet welcoming the user to NT was left on the keyboard to greet the user when they arrived on Monday. Users had been advised to attend training prior to conversion and the pamphlet also contained a refresher summarizing how to log in and how to use the new NT desktop.

The goal for the first weekend rollout was 50 machines. Systems accomplished 48 by Sunday evening after an exhausting weekend. The next day, the Systems Help Desk was inundated with calls. People could not log in. The technical representatives could not handle the load, and Systems staff had to circulate the floors to assist people. It was hectic, but after the early initial chaos and confusion, things settled down and people began to get comfortable with the new environment. Two more machines were completed early in the week to meet the target of 50 machines to be installed, but after this experience, management agreed to drop the number of machines to be converted at any one time to 25 machines.

Progress was continually and steadily made on the migration. Ideally, the process would have been to do this only a few times and to do large migrations to minimize the time and effect on everyone. Requiring the staff to work a full week in preparing machines and then working the weekend rolling out machines week after week, however, took a toll on them. Furthermore, while this was going on, the normal business of Windows 3.11, database and network support continued.

A number of factors limited the number of machines that could be converted. The experience on the first conversion weekend proved migrating too many machines could be overwhelming and disruptive. There were insufficient resources to do a large- scale change over. Logistical factors also precluded large migrations. Machines had to be pre-installed and had to be available before hand. Machines collected were held for one week before recycling back. Once the initial 50 new machines were fielded, the process depended upon trickling down previous users' machines for new configurations. Without sufficient resources, it was just not feasible to do any large-scale conversion at one time.

Instead, machines were steadily trudged out. This may have been for the best but it made the process longer and it was a constant strain on Systems. Everything took time. As mentioned earlier, the clean up process and review on users configuration took a lot of time.

Reviewing the users' disks took time. QA took time. One user was caught moving not only data but also games and software in the MYDATA directory, hoping Systems would not catch this and transfer it over to the new system. Other users who probably were too busy just copied their entire C directory into MYDATA. The process improved over the weeks.

The final step was to follow up on all the parts of the changeover. Calls were made to users from the DMDC Systems Help Desk asking if their setup was satisfactory. A survey was sent out. Discussions of the platform and progress of the migration were held at each weekly executive meeting. Interestingly enough, as the rollout neared completion, there was not an outcry of inability to work as some claimed when they heard only Systems would have local administrative privileges. There may be different reasons for this. It turned out in a majority of cases to be more a fear of loss than a reality of need. However in some cases, the resourceful individuals just figured out ways to beat the system. One employee used a Linux boot disk to gain control of the PC and then proceeded to reinstall NT over our standard system. He established himself as local administrator and locked Systems out. This became a strong source of contention with his management.

By the end of 1998, over a year after the first announcements of NT, the project was completed. Systems took time off during the Christmas holidays. Special Act

awards were presented to the Systems staff for all the extra work and the many long hours. A pizza party was given to the technical representatives. This was, however, actually not the end but just the beginning. There were issues on how to handle a host of fringe software. MS Exchange had to follow up this deployment. It was hoped the experience and lessons learned would facilitate the migrations and new conversions to follow.

VI. ANALYSIS OF DMDC NETWARE TO NT MIGRATION

This chapter provides an analysis of the case history presented in Chapter V. The NT implementation at DMDC was impacted by organizational, technical and project management factors. The analysis applies Stewart Stokes' Seven-Step Change Process and Todd Jick's Ten Commandments of Implementing Change to the DMDC NT implementation.

A. ORANIZATIONAL FACTORS

1. Change Management

The implementation of change within the workplace can be extremely complex. The variables of change include but are not limited to leadership, personnel, structure, and culture.

The selection of a clear strategy for change is crucial to success. Managers often see change as a simple decision process involving a series of a yes or no alternatives. While this may work in certain instances, a structured planning tool produces an increased chance of success. The Stokes Seven-Step Change process outlined in Chapter IV is one method that emphasizes the special challenges of technology-driven change. Management professor, Todd Jick, provides another example with his 10 Commandments of Implementing Change (Figure 6.2).

Jick's "commandments" were compiled as a checklist for managers about to implement organizational change, but it is interesting to see the similarities between the

two guidelines. Both authors advocate that management must understand the reasons for change and identify the benefits it will bring to the organization. This understanding must be clearly communicated to everyone in the organization so that there is a shared vision and common direction. Management should communicate, involve people and be honest. An implementation plan should be carefully developed. Once the change is implemented, it should be reviewed and reinforced. Jick warns that change management is not a simple step-by-step process easily accomplished by using a checklist. However, models for approaching a change process like his "10 Commandments" and Stokes' Seven-Steps provide managers with a list of things to consider. Without these models or checklists, which represent the experience and analysis of previous change efforts, a manager is left to learn all of these things "the hard way."

Systems did not have a structured change management approach to the NT migration. There was no formal analysis on impact, resistance, support or corporate culture. Technical issues were the primary focus of the DMDC NT implementation. However, the Chief of the Systems Department was aware that change should be managed. His planning included some steps to address change management issues like resistance to change, but without a more structured process some important steps were missed. This resulted in some of the problems encountered in DMDC's NT implementation project.

The 10 Commandments of Implementing Change

1. Analyze the organization and its need for change.
2. Create a shared vision and common direction.
3. Separate from the past.
4. Create a sense of urgency.
5. Support a strong leader role.
6. Line up political sponsorship.
7. Craft an implementation plan.
8. Develop enabling structures.
9. Communicate, involve people, and be honest.
10. Reinforce and institutionalize change.

Figure 6.2 "The 10 Commandments of Implementing Change" (Jick, 1997, p.195)

a. Forces Driving Change

In order for change to occur, people must feel they need the change. In the case of DMDC, everyone understood that the change to NT was good for the organization. Realizing this, Systems management underestimated the need to communicate with and reassure those impacted by the change. Some of Jick's Ten Commandments such as analyzing the need for change, separating from the past, and lining up political sponsorship were not considered for DMDC's NT migration.

b. Resistance to Change

There was little or no resistance to the change to NT at DMDC. However, there was resistance to the way Systems intended to implement NT. Systems wanted to use NT to enforce its network policies. Prior to NT the mechanisms to "lock down" the desktop to a standard configuration were not available. Systems spent many hours trouble shooting and fixing problems caused by users deleting or changing their desktop configurations. NT presented Systems with the opportunity to control the desktop configuration and eliminate one of their major trouble call areas. Many DMDC users

wanted the flexibility to configure their own desktop and resisted Systems' plan to eliminate this capability. DMDC and Systems Department management could have put more time and energy in communicating with users about why a standard desktop configuration was good for the organization.

Stokes says that the first step in the change process is to identify the forces for change and understand the threats and opportunities associated with the change. Individuals and organizational units may view the change from different perspectives. The perceived threats and opportunities can differ with each person or group. DMDC Systems did not recognize that its plan to restrict workstation configuration control could be a threat to some groups within the organization. The failure to recognize this lead to problems with the implementation.

Systems did recognize the need to create a shared vision. Early in the project, after management approved funding, a series of technology newsletters were published. These newsletters described the technology directions of the organization. The newsletters also explained the benefits of the new technology. The cost savings along with enhanced stability and reliability were emphasized. The newsletters explained that using DMDC's standard desktop configuration and standard suite of software reduced complexity and improved network reliability. In the past, programmers and developers had reconfigured their workstations to meet the needs of their own projects. This action was not a problem until the organization grew. Individual reconfiguration of workstations that conflicted with the network architecture now caused delays in production and even interrupted service for the entire network. DMDC's business was

information. DMDC could no longer afford the threat to network reliability that lack of access controls allowed.

The newsletters correspond to step three of Stokes' change process. DMDC Systems communicated, early in the process, the explicit benefits of the change to NT. With these newsletters, Systems also tried to create a sense of urgency, which corresponds to the Jick's Fourth Commandment. The newsletters were a good way to explain Systems' point of view. However, they did not go far enough, and did not allow a user feedback mechanism.

c. Corporate Culture

Separating from the past, however, was difficult. Many employees were attracted to DMDC because of its focus on individual performance and its flexible environment. The work emphasis was on outcome, and not the process. There were few rules and almost no bureaucratic procedures. People did whatever it took to get the job done. The corporate culture rewarded individual efforts. People volunteered to work many hours with no extra pay to complete work within incredibly short time frames. This "can do" spirit was rewarded by upper management.

However, as the network and technology environment grew the complexity of the networking environment no longer allowed everyone to "do their own thing".

Systems was rewarded for providing a reliable, fast network. The programmers and analysts were rewarded for getting product out as quickly as possible. These two goals were sometimes directly opposed. If the programmers had access to change a configuration "on the fly" to short-cut a network control, they could impact

network reliability. Systems implementation of controls and standards often cost the programmers time when they were under a tight time schedule.

d. Developing Enabling Structures

Systems had a number of initiatives to satisfy the Jick's Eighth Commandment to develop enabling structures. It created the Systems Help Desk in anticipation of the changeover to NT. A newsletter was also published to increase communication. Systems communicated with customer departments via meetings. Other Systems' efforts to ease the change for users and provide enabling structures were the Division technical representative program, the Early Adopter program and the "Welcome to NT" user pamphlet. Systems worked closely with the two types of DMDC users, knowledge workers and developers, to develop user profiles that would provide appropriate functions.

Systems could have developed more ways to increase two-way communications. Developers could have participated in the planning phase, which might have eased some of the later conflicts. Additional strategies should have been devised to include more participation and make the process less directive.

Systems' credibility was hurt when the process took longer than expected. Having newsletters and enabling structures work at the beginning. These change management processes build confidence. But if the process takes too long, they begin to work against you. Publicity, sharing information, enabling structures also build expectations. Systems lost credibility when it took such a long time to make the technology work. Systems failed to meet user expectations.

e. Change Management Applies to Everyone

Chapter IV notes that one should not assume the change recipients will be the only ones to resist change. Your own technical workers may resist the transition to a new system. This occurred with the NT migration project. Individual differences in philosophy compounded the technical difficulties and added to the delays. In the end, the team had to be reorganized.

Change management applies to everyone and open communications are needed with your project workers as well as the general staff.

f. Be Proactive in Training

Training is an important aspect. It is an important component in Jick's Seventh Commandment and in Stokes' sixth step.

The lesson learned regarding user training for NT caused Systems to modify its approach to user training for subsequent technical implementations. During the Exchange implementation that followed the NT project, Systems prepared a brief training session covering only the critical things needed to be operational. But rather than announce times for classes and passively wait for people who were too busy with their jobs to show up, Systems was proactive and went directly to the users. Each division had a weekly staff meeting. The Director of Systems coordinated with each Division Chief to hold a short session on technology changes and specifically on the new Exchange mail system. The short training session was part of their regular meeting. This was very successful and in several cases the sessions turned out longer as users became involved and asked a number of questions.

g. IT Philosophy

To most IT users, their world is the work they do and not the machines it is done on. Frequently, IT engineers are the ones fascinated with technology and are the ones who want all the flexibility and options. IT managers often label customers as apathetic or difficult when they do not attend IT training or do not clean off their disk drives prior to a migration. Managers with this perspective, forget that IT is not part of the customers' job. IT should be a tool to make their jobs easier.

More features and options simply represent confusion to many users. Customers of IT products want an easier or better way to do their work. They do not want new products bloated with "cute" features that do not represent a means of improving the way their work is accomplished. IT workers often have difficulty understanding things from the user's perspective. IT engineers should make the technology as powerful and useful as possible without creating a product that is a burden for customers to learn. Most users do not have the time or inclination to spend a great deal of time learning how to use an IT product. When using COTS software packages, the IT department can improve the usability of the product by knowing the features their customers need and configuring the software to provide only the useful features.

A good IT philosophy is that IT should be a work enhancing tool and not an extra task to IT customers. IT providers can offer a more useful tool by understanding the work their customers do and providing an IT configuration that clearly supports that work. Simplicity is key.

h. Management Support

Management support is one of the most critical components of project success. You cannot accomplish change management without upper management support. Get it early and keep communicating so upper management knows what is going on. Management support is key to handling all of the non-technical factors that parallel any IT project.

In this case, DMDC management supported the IT group and showed a lot patience. Management did not blame the Systems staff for the project's schedule slip. While they were anxious for the NT to be deployed, upper managers recognized how hard the team worked and the many hours that were put into the project. DMDC upper management supported Systems over many other factions and helped to create order from chaos in the cleanup process.

2. Conflict Management

It is important for management to realize that conflict is inevitable within organizations. Conflict is neither good nor bad. Conflict, like change, is simply a fact. The way conflict is managed determines its impact on the organization. If successfully managed, conflict can produce high quality solutions that lead to new, improved ways of doing business. The negative impacts of conflict in the workplace cannot be ignored. "The management of conflict usually entails maintaining a delicate balance between these positive and negative attributes." (Ware and Barnes, 1978)

When trying to manage a dispute, it is helpful to understand its origins. In the DMDC case, the standards conflict between Systems and Programming stems from the company's beginning. DMDC began as a small research firm comprised primarily of

engineers and scientists. There was no real hierarchical structure to the organization. The company grew, and management structures were implemented. However, the organizational culture continues to operate as a small, unstructured organization.

As DMDC grew, the need to implement standards and structure became apparent to some, and nowhere were they needed more than in the enterprise networking area. Management recognized that the network was a critical resource that needed standards and restricted access for its protection. However, management also needed the flexibility for programmers to do whatever they needed to get the job done.

a. Understanding the Situation: Cowboys versus Nazis

The attitudes each group had towards each other did not help the situation. Systems' perception was that programmers were "cowboys" whose unruly approach to getting their work done was a threat to the network. The programmers' perception was that the Systems staff was "Nazis" who wanted to tell everyone else how to do their job. There were substantive issues at the beginning of the conflict. It was System's job to make the network reliable for everyone's use. They needed to be the only ones with access to make network configuration changes in order to maintain network reliability. It was the programmer's job to produce fast results for OSD tasking. If the controls put in place by Systems slowed their ability to produce results, then the controls had to be eliminated. These substantive issues were not resolved and the conflict grew into an emotional one where each group saw the other in caricature, cowboys and Nazis.

Systems saw themselves as a service provider for the entire organization and the organization's customers. Programming saw themselves as the primary group

supporting DMDC's "can do" reputation. While both of these perspectives were based in fact, they limited each group's ability to see things from the other's point of view.

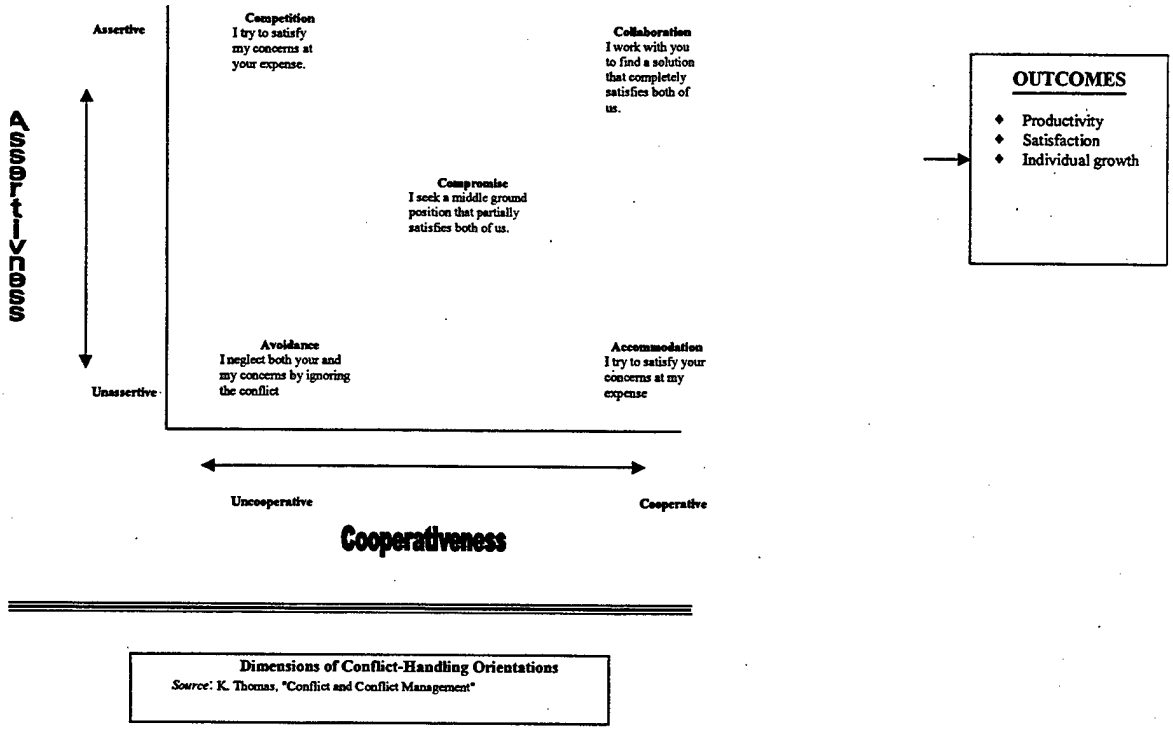
b. Thomas Conflict Resolution

K. Thomas describes five modes of conflict resolution. They are avoidance, competition, accommodation, compromise and collaboration. Exhibit 6.1 provides a graph of the dimensions of these conflict-handling modes. All modes can work given the situation. Avoidance may sound like a bad thing, but in situations where the conflict is trivial or the situation is obviously transient simply staying out of the other party's way is likely the best approach.

In the DMDC case, avoidance had been the situation before the change to NT. The programmers avoided Systems and made their changes in hopes that Systems was not aware. With the new technology to lock down desktops, the avoidance mode would no longer work.

Competition now was the conflict management mode of DMDC Systems and the programmers. If a competitive conflict such as the one at DMDC is allowed to run its course, it can have a significant negative impact on an organization's overall productivity. Dispute resolution experts, Jeanne M. Brett, Stephen B. Goldberg and William L. Ury focus on four criteria when evaluating a conflict management system. Those criteria are transaction costs, satisfaction with outcomes, effect on the relationship and recurrence of disputes (Brett et al., 1990).

Transaction costs are the time, money and emotional energy spent in the dispute, the misuse of resources, and the lost opportunities. At DMDC the dispute impacted productivity in Systems, in Programming and in the operational user



DMDC Management is in **Avoidance** mode.
Systems and Programming Departments are in **Competition** mode.
The goal is for Systems and Programming to be in **Collaboration** mode.

Figure 6.1 Five Conflict Handling Modes

departments. The impasse delayed the much-needed NT migration. The good will and team spirit that should have existed between the two groups would be destroyed by a long-term dispute. Brett, Goldberg and Ury warn that if the animosity exists for too long, it may be impossible for parties to ever get to a point of compromise much less collaboration.

Satisfaction with outcomes depends primarily on how the parties in dispute feel the resolution meets their needs, desires and concerns. The second issue is whether the parties believe the dispute resolution process is fair. The conflict between

Systems and the programmers had the potential for compromise. Collaboration between the two departments even was possible, if a common vision was developed and everyone felt that they were a valuable part of the process. This relates back to the recommendation in Chapter IV to determine a well-stated goal of where the change will take the organization and be sure everyone involved understands the goal. Crafting a vision could be a valuable part of the dispute resolution process. If all sides are given the opportunity to voice ideas and frustrations, general satisfaction with the outcome of the dispute resolution process will be more likely.

Effect on the relationship is an important criterion, for it deals with how well the parties will be able to work together in the future. The change from NetWare to NT is only one of many technical changes that will take place at DMDC. Systems and the programmers need to resolve their differences and learn to work together so that the negative feelings do not intensify to the point that every change effort will reach the same predictable impasse. Management has to stress and reward teamwork.

Recurrence of disputes looks at whether disputes once resolved stay resolved. If the same dispute arises between the same parties, it is likely that the dispute resolution process was inappropriate. If different parties have the same dispute, the original resolution process may work a second time. If the same parties encounter a different dispute, careful consideration should be given to how the two disputes differ. The facts surrounding each conflict should be understood before deciding on a dispute resolution approach. Given the nature of their jobs, the struggle between Systems and programmers will likely always produce conflicts. The key to successfully resolving those conflicts is the general understanding that everyone at DMDC is a valuable part of

a team that supports the organizational mission. The mission is best met when all parts of the organization work together rather than against each other.

B. TECHNICAL FACTORS

1. The Novell Factor

The decision to transition to NT and to keep Novell had the greatest impact on the project. Deciding to not do a forklift technology change made the project much more complicated. Given the lack of expertise and the difficulty with getting NT to replace all of NetWare's functions, Systems decision to retain NetWare and to transition into NT may have made sense. In hindsight, however, the entire process might have been easier if NT replaced Novell completely.

Part of the problem was that there were no guidelines or other models to look upon for help. There were stories of the difficulty at Xerox in trying to incorporate the two technologies. But Systems had no idea of how different the two systems were and how hard it would be to make them work together. Books like the Plumly reference on NetWare migration skirt the issues and do not provide the details that a hands-on, real implementation require. Books on Novell and NT tout their features, but there are no published details on problems and how to use both of them together while transitioning. There is some information on the Web but it is difficult to separate facts from prejudices. The Nowshadi reference on integrating NT and NetWare came out just this year. Combining NT and NetWare was a new experience but at that time DMDC did not know this.

Another problem was in the way DMDC managed technology. The design at DMDC was very specialized. The DMDC staff was expert in using the features of

NetWare to control access, licensing and to provide an organized system for upgrades. There was little information on this to be found elsewhere. Consequently, there was even less information to be found on how to do the NetWare tricks in NT. The Systems staff made the mistake of assuming they could do the same with NT. The struggle and the time expended in trying to have NT emulate the things the Systems group accomplished with Novell cost the project many hours.

Hindsight is 20-20. It may have been easier to implement NT without the time spent integrating with Novell. Systems believed it did not have sufficient NT expertise to risk dropping a successful network implementation and replacing it with an unknown. Even at the end of the project, conflicts made controlling the desktop an imperfect and incomplete solution.

DMDC cannot say for sure what would have happened if it had dropped Novell. Recently DFAS, in discussions with the authors, indicated Novell was still a better technology and they, like DMDC are deciding to keep both systems. A study on their design would be an interesting follow-up.

2. Microsoft Caveats

In order to implement controls and deliver software from NetWare servers DMDC made changes to the Windows NT registry. The registry contains all of the system configuration settings, and Microsoft does not typically support registry changes. Microsoft will not help you if the registry changes do not produce the intended results, and they may deny support for other problems if they know you have changed registry settings. However, Systems needed these changes to customize NT to manage the

desktop configurations. The engineering time to accomplish this was another factor that delayed the project.

Microsoft recognized the need for cloning machines in large-scale rollouts, but they expressed concerns about security and the SID. Each machine has its own identifier, called the secure id or SID. Initially, Microsoft would not support you if you cloned your machines using Ghost or Image Cast, because the SID would be copied and would no longer be unique. Later Microsoft provided support to large customers who used third-party cloning software and had a Microsoft Select Support contract.

DMDC used the cloning process. There is no practical way to install a large number of machines without cloning. Installing each machine manually would have been too labor intensive. DMDC added the SID after the install to make each machine unique and secure.

There are a number of products to assist in making the SID unique. Norton Ghost Walker and Systems Internals' perform this function. Microsoft also has now provided a tool called System Preparation, (SysPrep) to do this. (Edwards, 1999)

3. Marketing Hype

DMDC fell prey to the marketing hype and vendor promises. If possible, wait until a product has been proven before you install it. DMDC attempted to install NT before it was ready for "prime time." Many of the promised features and functionality did not work. The product does get better with each version, but prepare to handle some fairly serious technical hurdles if you must install a first version. You will suffer the consequences, as DMDC did while waiting for service packs and hot fixes.

C. PROJECT MANAGEMENT FACTORS

1. Underestimating Resources

a. Time

The successful completion of previous technical implementation projects and confidence in the technical talents of the Systems staff lead technical management to believe that the project was much simpler and required much less time and than it actually did. The size and scope of the project was underestimated during the planning phase and continued to be miscalculated throughout the life of the project. The Systems group's success with NetWare and previous large scale Windows 3.11 installs and migrations gave management the inaccurate idea that the NT implementation would require similar resources. As Yogi Berra would say, "You just don't know what you don't know".

The staff struggled attempting to implement functions in NT that were available in NetWare. For example, to make necessary upgrades, DMDC engineers used NetWare login scripts to capture control of a workstation at login time. This allowed them to determine the workstation software configuration to know which components needed to be installed. NT did not support this method. Microsoft recommended a separate Microsoft product, System Management Server (SMS), to accomplish the task. The Systems Department believed that it would be more difficult to learn SMS than to use NetWare login scripts. In addition, SMS would have required the purchase of another server and more software licenses.

Lack of NT experience and the fact that NT did not always work as advertised or provide equivalent NetWare functionality cost the implementation team many hours.

The following information may provide some perspectives for other NT migrations. DMDC took over a year of time, on average about three man-years in development, for a combined NT and Novell server environment and a controlled desktop environment. It took eight people working nights and weekends for three months to install NT on over 400 desktops.

b. Personnel

Although System's presentations to DMDC upper management garnered equipment resources, personnel resources were inadequate. The Systems team consisted of three people: a team leader, a systems engineer and a junior engineer. The network manager and a network systems administrator were enlisted for additional engineering support, but they were available only on a part-time basis. A three-member PC support team was drafted at different times for rollout support. Most members of this group were also fully engaged in other projects at the same time.

A senior on-site technical consultant said the normal process would be to contract an outside team to provide technical expertise, experience and the man-hours to do the deployment. The consultant observed that workers who had other full-time duties could not apply the time needed to successfully complete a major project. DMDC chose to use in-house personnel, because previous DMDC employee implementations were successful. DMDC saved money on personnel resources, but the lack of NT experience cost Systems and the organization in other ways. The commitment and perseverance of

the Systems staff brought the project to completion, but the difficulties encountered and long hours required took a high toll on the staff.

2. No Model

In managing a project, managers often rely on the histories of other similar implementations to estimate the time required to complete the project. DMDC began its NT migration process early in the life of NT 4.0. There were no guidelines to follow regarding reasonable timelines and resources requirements. IT publications and word of mouth indicated that many organizations encountered problems when converting to NT. DMDC seemed to have plenty of company in the problems department, but no success stories to learn from. The previous successful DMDC implementations of UNIX and Oracle had the benefit of a large body of implementation knowledge. NT, in many ways, represented new technology. Roadmaps to successful NT implementations did not exist.

3. Lack of training

Managing training is an important part of managing the project. NT training was available, and a few network engineers attended some training. However, there never seemed to be the time to send someone away for the recommended seven weeks of NT classes. In addition to the time constraint, NT training for Systems personnel was not a high priority, because they felt technically competent to handle the implementation without training. Their previous record with UNIX and Oracle lead the Systems engineers to believe they could "figure out" NT. They misjudged how different NT was from other technologies and how difficult it was to implement a technology without the benefit of published and anecdotal guidelines. Training was definitely a missing component. Training may have helped with the technical issues. However, as described

in Chapter III, the implementation of NT requires hands-on experience. The lack of training was a factor, but even with training there was no practical experience to guide employing the technology.

4. Coordination

The Systems Department did a good job coordinating with technical representatives in each functional division. This collaborative effort helped them to upgrade 400 workstations to NT with no data loss.

Systems failure to coordinate with the trainer cost them. Also, after the first group of workstations were upgraded to NT, there was much confusion. Users could not login. This was due to a failure to actively engage the staff on what would be happening and what they needed to know. The instructions were on the pamphlet that was left on the desktops for the people to see when they arrived the next day. But practically no one read them; they just called the Help Desk. This shortcoming was remedied on subsequent rollouts.

5. Implementation

Implementation went fairly smoothly. The key was in having everything coordinated beforehand. As described above, coordination was done fairly well. No data were lost. There were three backups for everyone's data. As a precaution, Systems also kept the user's workstation for an extra week before formatting it for someone else. In delivering over 400 machines, this extra insurance step had to be used only once. The machine was pulled out and the user recouped his data.

The biggest concern was user satisfaction. There was much consternation before implementation from users over their loss of the ability to change their workstations.

However, this turned out not to be the case after implementation. The situation worked itself out with both office automation staff as well as the programmers. The fear of loss was greater than the reality.

6. Management support

A key factor in the eventual success of the migration to NT at DMDC was management support. In other sections, the value of management support was explained. Management was extremely patient given that the estimated six-month project took well over a year to accomplish. Management supported Systems in conflicts with other functional divisions. Management also was aware of the problems and complexity in rolling out new technology.

D. CHAPTER SUMMARY

As the saying goes, "The best laid plans...". The Systems Department at DMDC approached the NT project with a good plan. They considered the human factors involved in any technology-driven change. They carefully planned the process of moving the data from the old to the new system to reduce the chances of data loss. They were veterans of other technical implementations and had a good record for producing results. There were many factors leading to the problems encountered at DMDC. No one group carried all of the blame and no one group was blameless. This story is another reminder that communication and human interaction are very important parts of a successful technical implementation. Chapter VII summarizes the key points and provides some lessons learned from DMDC's NetWare to NT conversion. It also includes a discussion of ways to avoid common project management mistakes.

THIS PAGE INTENTIONALLY LEFT BLANK

VII. LESSONS LEARNED AND CONCLUSION

There are technology issues and people issues associated with every technical implementation. Chapter III outlines the technical considerations of a NetWare to NT conversion. Chapter IV discusses the importance of change management (human factors) to the success of a technical project. Chapter V tells the story of DMDC's NetWare to NT conversion experience. Chapter VI is an analysis of the DMDC case study. The Seven-Step Change Process analytical framework is used to review DMDC's technical migration experience. In this final chapter of the thesis, a list of lessons learned is derived from the analysis in Chapter VI. In addition, recommendations for avoiding some common project management mistakes are provided.

A. NETWARE TO NT LESSONS LEARNED AT DMDC

1. Use One NOS

Convert all of your network functions to NT. It is too expensive to run NetWare for some things and NT for others. Attempting to integrate the two systems is difficult. You will need two types of NOS technical expertise. It is possible to have your staff trained in both, but the reality of under-staffed, over-worked DoD IT departments means that you cannot be as effective with two systems to support. The authors find this advice difficult to give, because NetWare is technically superior to NT in many ways. However, Microsoft will eventually catch up technically. NT is an operating system that adequately supports most LAN environments. Market trends indicate that NT will be the leading LAN OS for the foreseeable future.

2. Allocate Sufficient Time

Do not underestimate the amount of time it takes to complete a technical conversion as complex as moving a production environment from NetWare to NT. That is easy to say, but difficult to do. Make a careful time estimate. Then multiply your initial time estimate by three. If you complete the project within the original estimate, you are a hero. If you take longer than initially estimated you are the only one who knows. This advice is not dishonest. It is simply practical.

Time estimation for technical projects is extremely difficult given the number of variables associated with most implementations. Most people underestimate how long it takes to accomplish a complex project. (If you have ever written a thesis, you can relate.) In addition, IT managers often feel pressured into overly-optimistic time estimates by their management. Do not let this happen. You may be telling management something it does not want to hear when you deliver a more realistic time estimate. However, that is a much better thing to do than to tell management the project will not be completed on time. This was a big lesson learned for DMDC's Systems group; however, it is a lesson for project managers in general.

3. NT Requires More Hardware

Budget for more hardware to move to NT. You will need more servers, more memory and more disk space. NetWare supports more users per server than NT does. In addition to the primary server, you need separate equipment for functions such as the BDC, DHCP, WINS and DNS.

4. NT Requires Special Expertise

NetWare administrators need NT training to effectively complete a NetWare to NT conversion. If the budget allows, hire a technical consultant who has done NetWare to NT conversions. Make sure this is a "hands-on" technical talent and not just a "paper" MSCE.

B. PROJECT MANAGEMENT RECOMMENDATIONS

1. Get Management Support

Top management support is crucial. Be sure that your understanding of why the change is happening and your expectations for how the change will benefit the organization are aligned with those of upper management. Be realistic when establishing the project time-line. Research how long a NOS conversion to NT should take a site with your configuration. Avoid making "guesstimates", and remember technical projects generally take longer than anyone ever expects. Provide management with a clear time-line for each phase of the project. Do not let management's eagerness for the project to be finished make you under-estimate how much time it will take to do a quality job. Be direct and honest with management, even if you have to tell them something they do not want to hear.

2. "It's the People, Stupid."

Too often, information technology specialists look at only the technical factors. This paper and the case study highlight the need to include human factors. Devote time to understanding the impact of the intended change. Think of the effect on the stakeholders and how they will react. Think about who is likely to resist the change. What can you do about minimizing the impact? Study the organization and its corporate

culture and consider how you effect the change. Review Stokes Seven-Step process as well as Jick's Ten Commandments.

"When cold statistics and systems thinking threaten to cloud your judgement, remember this simple key to a long-lived business organism; people and culture count most." (Santosus, 1999) This is also true of IT implementations. People make or break projects. The stress and feelings of animosity that surround many IT projects happen because managers do not remember project management's human component. Somehow the nature of how people interact and work gets forgotten in the push to stay current with technology. If people concerns were at the top of project managers' plans rather than afterthoughts, the dismal IT project record would likely improve dramatically.

3. Communicate, Communicate, Communicate

Communication is critical. Communicate your understanding of the reasons for the change to your technical team. While they are involved in bringing the change to the organization, they will not always be supporters of the change plan. Successful teams have a common understanding of the work and a common set of goals.

Communicate with your management peers. Work to open lateral communication channels between departments. Include the people impacted by the change in the planning process. People do not like to be forced into major changes without being given the opportunity to provide lots of input.

Communicate with upper management. Obtaining management's support is an ongoing effort. It does not end, once they have agreed to back the project. You need to provide them timely project status reports. If you keep management informed, they can help you resolve issues that could delay the project.

Remember, there is no communication without listening. Listen to the ideas and concerns of your technicians, upper management, your management peers and the customers. When you start to do this, you will be better able to work together to develop a common understanding and a joint approach to implementing change.

4. Understand the Environment

The organizational environment should be factored into any technical implementation plan. The type of work the organization does, the organizational structure and culture are all components of its environment. The environment impacts the way the organization responds to change. Understanding the organization's mission, the way command and control is exercised and the unwritten cultural rules of the organization gives an IT project manager important information about the implementation approach that will work best.

5. Plan the Project

Planning may seem obvious, but many managers fail to do it or do it well. Put in writing what you are trying to do. The documentation will help you have a clearer idea of your objectives and provide a way to measure your progress. Involve change recipients in developing the implementation plan. Once a plan is developed and the implementation has started, compare the project's actual progress with the plan. Most plans change as unexpected events occur. Changing a plan is fine as long as the change makes sense in light of new information. Getting off track and abandoning a plan is not fine. Doing so is equivalent to never having developed a plan. Keep management informed of changes and actual versus planned project progress.

Carol Hildebrand's 1998 article, in *CIO Magazine*, "If At First You Don't Succeed" provides six project vital signs developed by Gopal K. Kapur, president of the Center for Project Management in San Ramon, California. Kapur advises project managers to know these six vital signs, define comfort thresholds at the beginning of a project, review the vital signs monthly and publicly post the results of each review. "Doing this will set up an environment where bad news can be conveyed early enough to head trouble off, " Kapur says (Hildebrand, 1998).

Kapur's project vital signs and his advice about reporting the status underscores the importance of communication in project management. The six project vital signs with Hildebrand's explanation of each are listed below.

(1) Status of the critical path. The critical path is a big-picture map of how the project should proceed, taking into consideration such factors as money, resources and time. Kapur recommends that if the status of the critical path is off by 15 percent, the team should try to figure out how to get back on track. He says that if the number rises to 20 percent, the team should adjust the scope, invest more money or reduce the quality of the end product. If the project is off by 25 percent, the project should be halted.

(2) Deliverable hit rate. The team's success at completing small project subtasks or deliverables.

(3) Milestone hit rate. Similar to the deliverable hit rate except it refers to the completion of major project tasks.

(4) Ratio of issues to deliverables. "Issues" is Kapur's word for unanswered questions, which could also be called problems. "If the number of issues exceeds the number of remaining deliverables, you don't have a plan anymore; you have a block of Swiss cheese, " he says.

(5) Planned budget versus actual budget. If a project goes too far over budget (using Kapur's 15/25 percent guideline), managers must reexamine the ROI to see whether the project costs are still justified by the benefits.

(6) Planned resources versus actual resources. This refers to items such as employees, hardware, software and time. Project managers should view this sign in the same way they view the budget sign. (Hildebrand, 1998)

C. CONCLUSION

Conversion from an old to a new IT system is a special kind of technical implementation. To use a house-building metaphor, it is often more difficult to remodel an existing house than it is to build a house from scratch. The same is true when an existing IT structure is "remodeled". Planning for things like running parallel systems, system cut-over, and data conversion are critical when migrating from an existing system to a new system. Protecting historical user data and timing a cut-over from the old to the new system are not issues, if the system is being implemented for the first time.

Changing network operating systems is not a simple process. This is especially true when the new NOS is as complex as NT. However, the process is doable and it will work. The good news is that historically, with Microsoft, it does get better.

Managing technology-driven change is not easy, but it can be done. The dismal record of IT implementations is due in large part to a failure to step back and understand what the business is about and then apply IT where it makes sense. Another major factor in IT's failure to live up to its potential, is the human component. IT managers need to move people issues to the top of their project plans.

In the case of an IT-21 mandated NetWare to NT conversion, an IT manager must understand why the decision was made to mandate a set of standards. The Navy and all of DOD can no longer maintain an array of IT infrastructures that are unable to seamlessly inter-operate. The costs in lost communication and overall productivity is entirely too great.

Information technology provides modern workers with marvelous tools to increase productivity and improve the workplace environment. While many believe that information technology has not lived up to its potential, most would agree that it has had a beneficial impact in some areas. Managing information technology projects is not a job for the faint-hearted. The complexity of most IT endeavors produces many issues (a.k.a. problems) for a project manager to resolve. Research, plan, communicate (talk and listen) and adopt a change implementation model that works for you. Success is never guaranteed, but doing these things will improve your overall IT project management success record.

LIST OF REFERENCES

Baltazar, "NOS Shootout", *PC Week,* May 10, 1999.

Berg, Glenn, *Networking Essentials,* New Riders, 1998.

Bharadwaj, Anandhi, Konsynski, Benn R., "Capturing the Intangibles", www.informationweek.com, September 22, 1997.

Blodgett, Mindy, "Hi, Technology!", www.cio.com/archive, February, 1998.

Bott, Ed, "Windows 2000", *PC Computing*, December 1998.

Boyce, Jim, *Windows NT Workstation, Advanced Technical Reference*, Que, 1996.

Boyer, Linda, "Novell Returns to Its Roots", *Netware Connection*, September 1998.

Byrne, Jason, "Active Directory or NDS", *Government Windows NT*, Volume 2, No. 1, Winter 1999.

Byrne, Jason, "Can Directories Keep NOSes In Sync?", *Government Computer News*, March 1998.

Cerbrowski, Vice Admiral Arthur K., Garstka, John J., "Network-Centric Warfare: Its Origin and Future", *Naval Institute Proceedings*, Annapolis, Maryland, 1997.

Dertouzos, Michael, "Creating the People's Computer", www.techreview.com, April 1997.

Dertouzos, Michael, *What Will Be*, HarperEdge, San Francisco, California, 1997.

Drews, James E., "NetWare5: NOS Battle Renews", *Network Computing Online,* www.nwc.com/902/902sp1.html, February 1, 1998.

Drew, James, "Integrating Netware and Windows NT", *Network Computing Online,* http://www.nwc.com/911/911wsl.html

Edwards, Mark, "Support for Cloned Systems, Microsoft's New Sysprep Tool", *Windows NT Magazine,* April 1999.

Field, Tom, "When Bad Things Happen to Good Projects", *CIO Magazine*, October, 15, 1997.

Hammer, Michael, "Back To The Future", *Computerworld,* 1987.

Hammond, Mark, "NOS Crossroads", *PC Week*, May 10, 1999.

Harbaugh, Logan, "NetWare 5: Substance Matters", *InformationWeek Online,* http://www.informationweek.com/708/08olntw2.htm, November 9, 1998.

Hayes, Heather, "Risk Management", Hard Copy@civic.com, www.civic.com, October 1998.

Jansen, Erik, "Organizational Structure That Works" handout from MN3105.

Jennings, Roger, *Using Windows NT Server 4*, Que, 1996.

Jick, Todd D., *Managing Change*, Irwin/McGraw Hill, 1993.

Johnston, Stuart, "Windows 2000", *Information Week*, p. 46, November 2, 1998.

Kessler, Gary and Monaghan, Carol, "NT and DHCP", *Windows NT*, May 1999.

Korzeniowski, Paul, *Windows NT versus Netware*, Computer Technology Research Corp, 1996.

Kotter, John P., Heskett, James L., *Corporate Culture and Performance*, The Free Press, Don Mills, Ontario, 1992.

Lawrence, Bill et al, *Using Netware 4.1*, Que, 1995.

Lewis, Ted G., *The Friction-Free Economy*, HarperCollins Publishers, New York, New York, 1997.

Markus, Lynne M., Benjamin, Robert I., "Are you gambling on a magic bullet?", *Computerworld*, October 20, 1997.

Microsoft, "Content Management Features", *Windows NT Server*, http://www.microsoft.com/NTServer/web/exec/overview/FeatContMgmt.asp

Microsoft, "File and Print Services", *Windows 2000 Server*, www.microsoft.com/windows/server/Overview/features/fileprint.asp, April 19, 1999.

Microsoft, "ITSEC Rating Confirms Security of Windows NT 4.0",http://www.microsoft.com/presspass/press/1999/Apr99/UKSecurPR.htm.

Microsoft "NT 5 Features", http://www.microsoft.com/windows/server/Overview/features/fileprint.asp

Microsoft "Web Content Management Features", http://www.microsoft.com/NTServer/web/exec/overview/FeatContMgmt.asp

Microsoft, "Web Services",http://www.microsoft.com/ntserver/web/exec/overview.asp

Milne, Jay "State of the NOS", *Network Computing*, February 1, 1998.

Minas, Mark, "SP4's Profile Quota Manager", *Windows NT Magazine*, April 1999.

Nowshadi, Farshad, *Managing Netware*, Addison-Wesley, 1994.

Nowshadi, Farshad and Norman Buskell, *Managing Windows NT / Netware Integration*, Addison Wesley, 1999.

Peters, Tom, "Reinventing the World", *CIO Magazine*, September 1, 1998.

Plumley, Sue, *Migrating from Novell Netware to Windows NT Server 4*, Wiley and Sons, Inc, 1997.

Russell, Deborah and Gangemim G.T., *Computer Security Basics,* O'Reilly & Associates, 1991.

Russinovich, Mark, "Inside the Registry", *Windows NT*, May 1999.

Sant'Angelo, Rick, *Netware Unleashed*, Sams Publishing, 1994.

Sheesley, John, "NDS for NT 2.0 – Connecting NetWare and Windows NT", http://www.zdjournals.com/inw/9904/inw9941.htm

Stokes, Stewart L. Jr., *Controlling the Future: Managing Technology-Driven Change*, QED Information Sciences, Inc., 1991.

Strebe, Matthew, et. Al, *MCSE: NT Server 4 Study Guide*, Sybex, 1997.

Thomas, K., "Conflict and Conflict Management," *Handbook of Industrial and Organizational Psychology*, p. 900, 1976.

Tittel, Ed, LANWright Consultants http://www.lanw.com, May 13, 1999.

Walker, Richard, "Firewalls", *Government Computer News*, May 10, 1999.

Wittmann, Art, "NT 5.0: Everything but the Kitchen Sink," *CMP Net*, http://w.nwc.com/921/921fl.htm

Wyatt, Allen, *Optimizing Windows 95*, IDG Books, 1996.

Web site for NT security hacking: http://www.L0pht.com

ZD Market Intelligence, "Netware No Longer Dominates: NT Takes the Lead in Installed LAN OS", ZDInfoBeads, September 1998, URL http://www/ci.infobeads.com/INSIDER/PAGES/TOPICS/NT/NT_Netware

THIS PAGE INTENTIONALLY LEFT BLANK

INITIAL DISTRIBUTION LIST

No. Copies

1. Defense Technical Information Center 2
   8725 John J. Kingman Rd., STE 0944
   Ft. Belvoir, VA 22060-6218

2. Dudley Knox Library 2
   Naval Postgraduate School
   411 Dyer Rd.
   Monterey, CA 93943-5101

3. Douglas Brinkley, Code SM/Bi 1
   Department of Systems Management
   Naval Postgraduate School
   Monterey, CA 93943

4. Professor Erik Jansen, Code SM/Ek 1
   Department of Systems Management
   Naval Postgraduate School
   Monterey, CA 93943

5. Professor Mark Nissen, Code SM/Ni 1
   Department of Systems Management
   Naval Postgraduate School
   Monterey, CA 93943

6. Janet Scruggs 1
   Office of Naval Intelligence
   4251 Suitland Road
   Washington, DC 20395-0002

7. Michael Yee 1
   Defense Manpower Data Center
   400 Gigling Road
   Seaside, CA 93955-6771